Guia do administrador

AWS Client VPN

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Client VPN: Guia do administrador

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

O que AWS Client VPNé ... 1
Recursos da Client VPN ... 1
Componentes do VPN do Cliente ... 2
Trabalhar com o Cliente VPN ... 3
Definição de preço para Client VPN ... 4
Regras e práticas recomendadas ... 5
Requisitos de rede e largura de banda ... 6
Configuração de sub-rede e VPC ... 7
Autenticação e segurança ... 7
Requisitos de conexão e DNS ... 8
Limitações e restrições ... 8
Como o VPN do Cliente funciona ... 9
Cenários e exemplos ... 10
Autenticação de cliente ... 22
Autenticação do Active Directory ... 23
Autenticação mútua ... 23
Single Sign-On (autenticação federada baseada em SAML 2.0) ... 29
Autorização do cliente ... 36
Grupos de segurança ... 36
Autorização com base em rede ... 36
Crie uma regra de grupo de segurança de endpoint ... 37
Autorização de conexão ... 38
Requisitos e considerações ... 38
Interface do Lambda ... 39
Utilize o manipulador de conexão do cliente para avaliação da postura ... 41
Habilitar o manipulador de conexão do cliente ... 41
Função vinculada ao serviço ... 42
Monitore falhas de autorização de conexão ... 42
Client VPN de túnel dividido ... 42
Benefícios do túnel dividido ... 43
Considerações sobre roteamento ... 43
Habilitar o túnel dividido ... 44
Registro em log de conexão ... 44
Entradas de log de conexão ... 45

Considerações sobre dimensionamento ... 47
Conceitos básicos da Client VPN ... 49
Pré-requisitos ... 50
Etapa 1: gerar chaves e certificados de servidor e cliente ... 50
Etapa 2: Criar um endpoint da Client VPN ... 50
Etapa 3: associar uma rede de destino ... 52
Etapa 4: adicionar uma regra de autorização para a VPC ... 53
Etapa 5: conceder acesso à Internet ... 53
Etapa 6: verificar os requisitos do grupo de segurança ... 54
Etapa 7: baixar o arquivo de configuração do endpoint da VPN do cliente ... 54
Etapa 8: conectar-se ao endpoint da VPN do cliente ... 55
Trabalhar com o Cliente VPN ... 56
Acesso ao portal de autoatendimento ... 57
Regras de autorização ... 58
Principais pontos ... 58
Cenários de exemplo ... 59
Adicionar uma regra de autorização ... 69
Remover uma regra de autorização ... 71
Visualizar regras de autorização do ... 71
Listas de revogação de certificados de cliente ... 72
Gerar uma lista de revogação de certificados de cliente ... 72
Importar uma lista de revogação de certificados de cliente ... 74
Exportar uma lista de revogação de certificados de cliente ... 75
Conexões de cliente ... 76
Visualizar conexões com de clientes ... 76
Encerrar uma conexão de cliente ... 77
Banners de login do cliente ... 77
Criação de banners ... 77
Configurar um banner de login do cliente para um endpoint existente ... 78
Desativar um banner de login do cliente para um endpoint ... 78
Modificar o texto do banner existente ... 79
Visualizar banner de login configurado atualmente ... 80
Trabalhando com o Client Route Enforcement ... 80
Requisitos ... 80
Conflitos de roteamento ... 81
Considerações ... 81

Ativar a aplicação da rota do cliente ... 83
Desativar a fiscalização de rotas do cliente ... 83
Endpoints ... 84
Requisitos para criar endpoints da Client VPN ... 84
Modificação do endpoint ... 84
Crie um endpoint do ... 86
Visualizar endpoints do ... 89
Modificar um endpoint do ... 90
Excluir um endpoint ... 92
Logs de conexão ... 93
Habilitar o registro em log de conexão para um novo endpoint do ... 94
Habilitar o registro em log de conexão para um endpoint do existente ... 95
Visualizar logs de conexão do ... 95
Desativar o log de conexão do ... 96
Exportação de arquivo de configuração do cliente ... 97
Exportar o arquivo do de configuração do cliente ... 98
Adicione o certificado de cliente e as informações principais para autenticação mútua ... 98
Rotas ... 99
Considerações sobre o uso do túnel dividido em endpoints da Client VPN ... 100
Criar uma rota de endpoint do ... 100
Visualizar rotas de endpoint do ... 101
Excluir uma rota de endpoint do ... 102
Redes de destino ... 102
Requisitos para criar uma rede de destino ... 102
Associar uma rede de destino a um endpoint do ... 104
Aplicar um grupo de segurança a uma rede de destino ... 104
Visualizar redes de destino do ... 105
Desassociar uma rede de destino de um endpoint ... 105
Duração máxima da sessão VPN ... 106
Configure a sessão VPN máxima durante a criação de um endpoint ... 107
Visualizar a duração máxima da sessão VPN atual do ... 107
Modificar a duração máxima da sessão VPN ... 108
Segurança ... 109
Proteção de dados ... 110
Criptografia em trânsito ... 111
Privacidade do tráfego entre redes ... 111

Gerenciamento de identidade e acesso ... 112
Público ... 112
Autenticação com identidades ... 113
Gerenciar o acesso usando políticas ... 116
Como AWS Client VPN funciona com o IAM ... 119
Exemplos de políticas baseadas em identidade ... 125
Solução de problemas ... 128
Uso de perfis vinculados ao serviço ... 130
Resiliência ... 133
Várias redes de destino para alta disponibilidade ... 134
Segurança da infraestrutura ... 134
Práticas recomendadas ... 135
IPv6 considerações ... 136
Monitorar a Client VPN ... 138
CloudWatch métricas ... 139
Exibir CloudWatch métricas ... 141
Cotas ... 143
Cotas da Client VPN ... 143
Cotas de usuários e grupos ... 144
Considerações gerais ... 144
Solução de problemas ... 145
Não é possível resolver o nome DNS do endpoint da Client VPN ... 146
O tráfego não está sendo dividido entre as sub-redes ... 146
Regras de autorização para grupos do Active Directory não funcionando conforme esperado ... 148
Os clientes não podem acessar uma VPC emparelhada, o Amazon S3 ou a Internet ... 149
O acesso a uma VPC emparelhada, ao Amazon S3 ou à Internet está intermitente ... 152
O software-cliente retorna erro TLS ... 153
O software-cliente retorna erros de nome de usuário e senha — autenticação do Active Directory ... 154
O software-cliente retorna erros de nome de usuário e senha — autenticação federada ... 155
Os clientes não conseguem se conectar – autenticação mútua ... 155
O cliente retorna um erro de credenciais que excede o tamanho máximo – autenticação federada ... 156
O cliente não abre o navegador — autenticação federada ... 156
O cliente não retorna erro de portas disponíveis — autenticação federada ... 157
Conexão VPN encerrada devido à incompatibilidade de IP ... 157

O tráfego de roteamento para a LAN não está funcionando conforme o esperado 158
Verificar o limite de largura de banda para um endpoint do 158
Conectividade de túnel Client VPN 159
Pré-requisitos de conectividade de rede 159
Verifique o status do endpoint do Client VPN 160
Verifique as conexões do cliente 160
Verifique a autenticação do cliente 161
Verifique as regras de autorização 161
Validar rotas do Client VPN 162
Verifique os grupos de segurança e a rede ACLs 162
Teste a conectividade do cliente 163
Diagnosticar o dispositivo cliente 163
Solucionar problemas de resolução de DNS 164
Solucionar problemas de desempenho 164
Monitore as métricas do Client VPN 164
Verifique os registros do Client VPN 165
Problemas e soluções comuns de 165
Histórico de documentos 168
..... clxxi

O que AWS Client VPNé

AWS Client VPN é um serviço VPN gerenciado baseado em cliente que permite acessar com segurança seus AWS recursos e recursos em sua rede local. com a Client VPN, você pode acessar seus recursos de qualquer local usando um cliente de VPN com base no OpenVPN.

Tópicos

- Recursos da Client VPN
- Componentes do VPN do Cliente
- Trabalhar com o Cliente VPN
- Definição de preço para Client VPN
- Regras e práticas recomendadas para utilizar o AWS Client VPN

Recursos da Client VPN

O VPN do Cliente oferece os seguintes recursos e funcionalidades:

- Conexões seguras: — fornece uma conexão TLS segura de qualquer local usando o cliente OpenVPN.
- Serviço gerenciado — É um serviço AWS gerenciado, portanto, elimina a carga operacional de implantar e gerenciar uma solução VPN de acesso remoto de terceiros.
- Alta disponibilidade e elasticidade — Ele é escalado automaticamente de acordo com o número de usuários conectados aos seus AWS recursos e aos recursos locais.
- Autenticação: compatível com autenticação de cliente usando o Active Directory, a autenticação federada e a autenticação baseada em certificado.
- Controle granular: permite implementar controles de segurança personalizados definindo regras de acesso baseadas na rede. Essas regras podem ser configuradas na granularidade dos grupos do Active Directory. Você também pode implementar o controle de acesso usando grupos de segurança.
- Facilidade de uso — Ele permite que você acesse seus AWS recursos e recursos locais usando um único túnel VPN.

- Capacidade de gerenciamento: permite que você visualize logs de conexão, que fornecem detalhes sobre tentativas de conexão de clientes. Você também pode gerenciar conexões de clientes ativas, com a capacidade de encerrá-las.
- Integração profunda — Ela se integra aos AWS serviços existentes, incluindo AWS Directory Service o Amazon VPC.

Componentes do VPN do Cliente

Veja a seguir os principais conceitos de VPN do Cliente:

Endpoint do cliente VPN

O endpoint do cliente VPN é o recurso que você cria e configura para habilitar e gerenciar sessões do cliente VPN. É o ponto de término de todas as sessões da VPN do cliente.

Rede de destino

Uma rede de destino é a rede que você associa a um endpoint do cliente VPN. Uma sub-rede de uma VPC é uma rede de destino. Associar uma sub-rede a um endpoint do cliente VPN permite estabelecer sessões de VPN. É possível associar várias sub-redes a um endpoint do cliente VPN para alta disponibilidade. Todas as sub-redes devem ser provenientes da mesma VPC. Cada sub-rede deve pertencer a uma Zona de disponibilidade diferente.

Rota

Cada endpoint do cliente VPN tem uma tabela de rotas que descreve as rotas de redes de destino disponíveis. Cada rota na tabela de rotas especifica o caminho do tráfego para recursos ou redes específicos.

Regras de autorização

Uma regra de autorização restringe os usuários que podem acessar uma rede. Para uma rede especificada, configure o grupo do provedor de identidade (IdP) ou do Active Directory que tem permissão de acesso. Somente os usuários pertencentes a esse grupo podem acessar a rede especificada. Por padrão, não há regras de autorização, e você deve configurá-las para permitir que os usuários acessem recursos e redes.

Cliente

O usuário final que se conecta ao endpoint do cliente VPN para estabelecer uma sessão de VPN. Para estabelecerem uma sessão de VPN, os usuários finais precisam baixar um cliente OpenVPN e usar o arquivo de configuração do VPN do Cliente que você criou.

Intervalo CIDR do cliente

Um intervalo de endereços IP do qual devem ser atribuídos endereços IP do cliente. Cada conexão com o endpoint do cliente VPN recebe um endereço IP exclusivo do intervalo CIDR do cliente. Você escolhe o intervalo CIDR do cliente, por exemplo, `10.2.0.0/16`.

Portas VPN do cliente

AWS Client VPN suporta as portas 443 e 1194 para TCP e UDP. O padrão é a porta 443.

Interfaces de rede da Client VPN

Quando você associa uma sub-rede ao endpoint do cliente VPN, criamos interfaces de rede do VPN do Cliente nessa sub-rede. O tráfego enviado para a VPC do endpoint do cliente VPN é enviado por meio de uma interface de rede do VPN do Cliente. A conversão de endereço de rede de origem (SNAT) é aplicada e o endereço IP de origem do intervalo CIDR do cliente é convertido no endereço IP da interface de rede do VPN do Cliente.

Registro em log de conexão

É possível habilitar o registro em log de conexão para o endpoint do cliente VPN a fim de registrar eventos de conexão. É possível usar essas informações para executar perícia, analisar como seu endpoint da cliente VPN está sendo usado ou depurar problemas de conexão.

Portal de autoatendimento

Um Cliente VPN fornece um portal de autoatendimento como uma página da Web para que os usuários finais baixem a versão mais recente do AWS VPN Desktop Client e a versão mais recente do arquivo de configuração do endpoint do Cliente VPN, que contém as configurações necessárias para se conectar ao endpoint. O administrador do endpoint da Client VPN pode habilitar ou desabilitar o portal de autoatendimento para o endpoint da Client VPN. O portal de autoatendimento é um serviço global apoiado por pilhas de serviços nas seguintes regiões: Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Tóquio), Europa (Irlanda) e AWS GovCloud (Oeste dos EUA).

Trabalhar com o Cliente VPN

É possível trabalhar com a Client VPN de qualquer uma das seguintes formas:

AWS Management Console

O console fornece uma interface de usuário baseada na Web para a Client VPN. Se você se inscreveu em um Conta da AWS, você pode entrar no console da Amazon VPC e selecionar Client VPN no painel de navegação.

AWS Command Line Interface (AWS CLI)

AWS CLI Fornece acesso direto ao público do Client VPN APIs. É compatível com Windows, macOS e Linux. Para obter mais informações sobre como começar a usar o AWS CLI, consulte o Guia AWS Command Line Interface do usuário. Para obter mais informações sobre os comandos do Client VPN, consulte a EC2 seção da Amazon EC2 Command Line Reference.

AWS Tools for Windows PowerShell

AWS fornece comandos para um amplo conjunto de AWS ofertas para quem cria scripts no PowerShell ambiente. Para obter mais informações sobre os conceitos básicos do AWS Tools for Windows PowerShell, consulte o Guia do usuário do AWS Tools for Windows PowerShell. Para obter mais informações sobre cmdlets para a cliente VPN, consulte Referência de cmdlets do AWS Tools for Windows PowerShell.

API de consulta

A API de consulta HTTPS do Client VPN fornece acesso programático ao Client VPN e. AWS A API de consulta HTTPS permite que você execute solicitações HTTPS diretamente para o serviço. Quando você usa a API HTTPS, deve incluir código para assinar digitalmente solicitações usando suas credenciais. Para obter mais informações, consulte Ações do AWS Client VPN.

Definição de preço para Client VPN

Você é cobrado por cada associação de endpoint e cada conexão VPN por hora. Para obter mais informações, consulte Preços do AWS Client VPN.

Você é cobrado pela transferência de dados da Amazon EC2 para a Internet. Para obter mais informações, consulte Transferência de dados na página de preços EC2 sob demanda da Amazon.

Se você ativar o registro de conexão para seu endpoint do Client VPN, deverá criar um grupo de CloudWatch registros de registros em sua conta. Aplicam-se cobranças ao uso de grupos de log. Para obter mais informações, consulte os CloudWatch preços da Amazon (em Nível pago, escolha Logs).

Se você habilitar o manipulador de conexão do cliente para o endpoint do cliente VPN, será necessário criar e invocar uma função do Lambda. Cobranças são aplicadas ao invocar funções do Lambda. Para obter mais informações, consulte Preços do AWS Lambda.

Os Endpoints da Client VPN estão associados a uma rede de destino, que é uma sub-rede em uma VPC. Se essa VPC tiver um Internet Gateway, associaremos endereços IP elásticos às interfaces de rede elástica do Client VPN ()ENIs. Esses endereços IP elásticos são cobrados como IPv4 endereços públicos em uso. Para obter mais informações, consulte a guia IPv4 Endereço público na página de preços da VPC.

> **Note**
>
> Os endpoints do Client VPN exigem endereços IP elásticos quando associados a uma sub-rede VPC que tenha um Internet Gateway, pois EIPs eles permitem conectividade direta com a Internet para clientes VPN. Ao se conectar por meio de um endpoint Client VPN, eles precisam de um endereço IP público para se comunicar com os recursos da Internet. A Elastic IPs atende a esse propósito fornecendo um endpoint consistente voltado para o público. Eles EIPs estão conectados às interfaces de rede elástica (ENIs) do Client VPN e são essenciais para manter o acesso estável e seguro à Internet para clientes VPN e, ao mesmo tempo, garantir o roteamento adequado do tráfego. Como esses endereços IP elásticos são alocados e usados ativamente para o serviço Client VPN, eles são AWS cobrados como IPv4 endereços públicos em uso, seguindo seu modelo de preços padrão para alocação e associação. EIPs

Regras e práticas recomendadas para utilizar o AWS Client VPN

As seções a seguir descrevem as regras e as melhores práticas de uso AWS Client VPN:

Tópicos

- Requisitos de rede e largura de banda
- Configuração de sub-rede e VPC
- Autenticação e segurança
- Requisitos de conexão e DNS
- Limitações e restrições

Requisitos de rede e largura de banda

- AWS Client VPN é um serviço totalmente gerenciado que se expande automaticamente para acomodar conexões adicionais de usuários e requisitos de largura de banda. Cada conexão de usuário tem uma largura de banda básica máxima de 50 Mbps. Você pode solicitar um aumento por meio do AWS Support, se necessário. A largura de banda real experimentada pelos usuários que se conectam por meio de um endpoint Client VPN pode variar com base em vários fatores. Esses fatores incluem tamanho do pacote, composição do tráfego (combinação TCP/UDP), políticas de rede (modelagem ou limitação) em redes intermediárias, condições da Internet, requisitos específicos do aplicativo e o número total de conexões simultâneas de usuários.
- Os intervalos CIDR de cliente não podem se sobrepor ao CIDR local da VPC na qual a sub-rede associada está localizada ou a quaisquer rotas adicionadas manualmente à tabela de rotas do endpoint da Client VPN.
- Os intervalos de CIDRs do cliente devem ter um tamanho de bloco de pelo menos /22 e não deve ser maior que /12.
- Uma parte dos endereços no intervalo de CIDR do cliente é usada para oferecer compatibilidade com o modelo de disponibilidade do endpoint do cliente VPN e não pode ser atribuída aos clientes. Portanto, é recomendável atribuir um bloco CIDR que contenha o dobro do número de endereços IP necessários para habilitar o número máximo de conexões simultâneas às quais você planeja oferecer compatibilidade no endpoint do cliente VPN.
- O intervalo CIDR do cliente não pode ser alterado depois de criar o endpoint do cliente VPN.
- O Client VPN suporta somente IPv4 tráfego. Consulte IPv6 considerações para AWS Client VPN para obter detalhes sobre IPv6.
- O Client VPN executa a Tradução de Endereços de Rede (NAT). Quando um cliente se conecta por meio do Client VPN:
  - O endereço IP de origem é traduzido para o endereço IP do endpoint do Client VPN.
  - O número da porta de origem original do cliente permanece inalterado.
- O Client VPN executa Port Address Translation (PAT) somente quando usuários simultâneos estão se conectando ao mesmo destino. A tradução de portas é automática e necessária para oferecer suporte a várias conexões simultâneas por meio do mesmo endpoint de VPN.
  - Para a tradução do IP de origem, o endereço IP de origem é traduzido para o endereço IP da VPN do cliente.
  - Para a tradução da porta de origem para conexões de um único cliente, o número da porta de origem original pode permanecer inalterado.

- Para a tradução da porta de origem para vários clientes que se conectam ao mesmo destino (o mesmo endereço IP e porta de destino), o Client VPN realiza a conversão de portas para garantir conexões exclusivas.

Por exemplo, quando dois clientes, cliente 1 e cliente 2, se conectam ao mesmo servidor e porta de destino por meio de um endpoint Client VPN:

- A porta original do cliente 1 — por exemplo, `9999` — pode ser traduzida para uma porta diferente — por exemplo, porta`4306`.
- A porta original do cliente 2 — por exemplo, `9999` — pode ser traduzida em uma porta exclusiva diferente do cliente 1 — por exemplo, porta`63922`.

Configuração de sub-rede e VPC

- As sub-redes associadas a um endpoint do cliente VPN deve estar na mesma VPC.
- Você não pode associar várias sub-redes da mesma Zona de disponibilidade a um endpoint do cliente VPN.
- Um endpoint do cliente VPN não é compatível com associações de sub-rede em uma VPC de locação dedicada.

Autenticação e segurança

- O portal de autoatendimento não está disponível para clientes autenticados usando a autenticação mútua.
- Se a autenticação multifator (MFA) estiver desabilitada para o Active Directory, as senhas de usuário não poderão estar no formato a seguir.

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- Os certificados usados no AWS Client VPN devem seguir a RFC 5280: Certificado de infraestrutura de chave pública X.509 da Internet e perfil da lista de revogação de certificados (CRL), incluindo as extensões de certificado especificadas na seção 4.2 do memorando.
- Nomes de usuário com caracteres especiais podem causar erros de conexão.

Requisitos de conexão e DNS

- Não é recomendável se conectar a um endpoint da Client VPN usando endereços IP. Como a Client VPN é um serviço gerenciado, você ocasionalmente verá alterações nos endereços IP aos quais o nome DNS resolve. Além disso, você verá as interfaces de rede do Client VPN excluídas e recriadas em seus CloudTrail registros. É recomendável se conectar ao endpoint da Client VPN usando o nome DNS fornecido.
- O serviça Client VPN exige que o endereço IP ao qual o cliente está conectado corresponda ao IP para o qual o nome DNS do endpoint da Client VPN resolve. Em outras palavras, se você definir um registro DNS personalizado para o endpoint Client VPN e encaminhar o tráfego para o endereço IP real para o qual o nome DNS do endpoint é resolvido, essa configuração não funcionará usando clientes fornecidos recentemente. AWS Esta regra foi adicionada para mitigar um ataque de IP do servidor, conforme descrito aqui: TunnelCrack.
- Você pode usar um cliente AWS fornecido para se conectar a várias sessões simultâneas de DNS. No entanto, para que a resolução de nomes funcione corretamente, os servidores DNS de todas as conexões devem ter registros sincronizados.
- O serviço da Client VPN exige que os intervalos de endereços IP da rede local (LAN) dos dispositivos clientes estejam dentro dos seguintes intervalos de endereços IP privados padrão: `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16` ou `169.254.0.0/16`. Se for detectado que o intervalo de endereços da LAN do cliente está fora dos intervalos acima, o endpoint da Client VPN enviará automaticamente a diretiva OpenVPN “redirect-gateway block-local” para o cliente, forçando todo o tráfego da LAN para a VPN. Portanto, se você precisar de acesso à LAN durante as conexões VPN, é recomendável usar os intervalos de endereços convencionais listados acima para sua LAN. Esta regra é aplicada para mitigar as chances de um ataque local na rede, conforme descrito aqui:. TunnelCrack

Limitações e restrições

- Atualmente, o encaminhamento de IP não é suportado ao usar o aplicativo AWS Client VPN de desktop. O encaminhamento de IP é compatível com outros clientes.
- A Client VPN não é compatível com a replicação de várias regiões no AWS Managed Microsoft AD. O endpoint do Client VPN deve estar na mesma região do AWS Managed Microsoft AD recurso.
- Não será possível estabelecer uma conexão de VPN em um computador se houver vários usuários conectados ao sistema operacional.

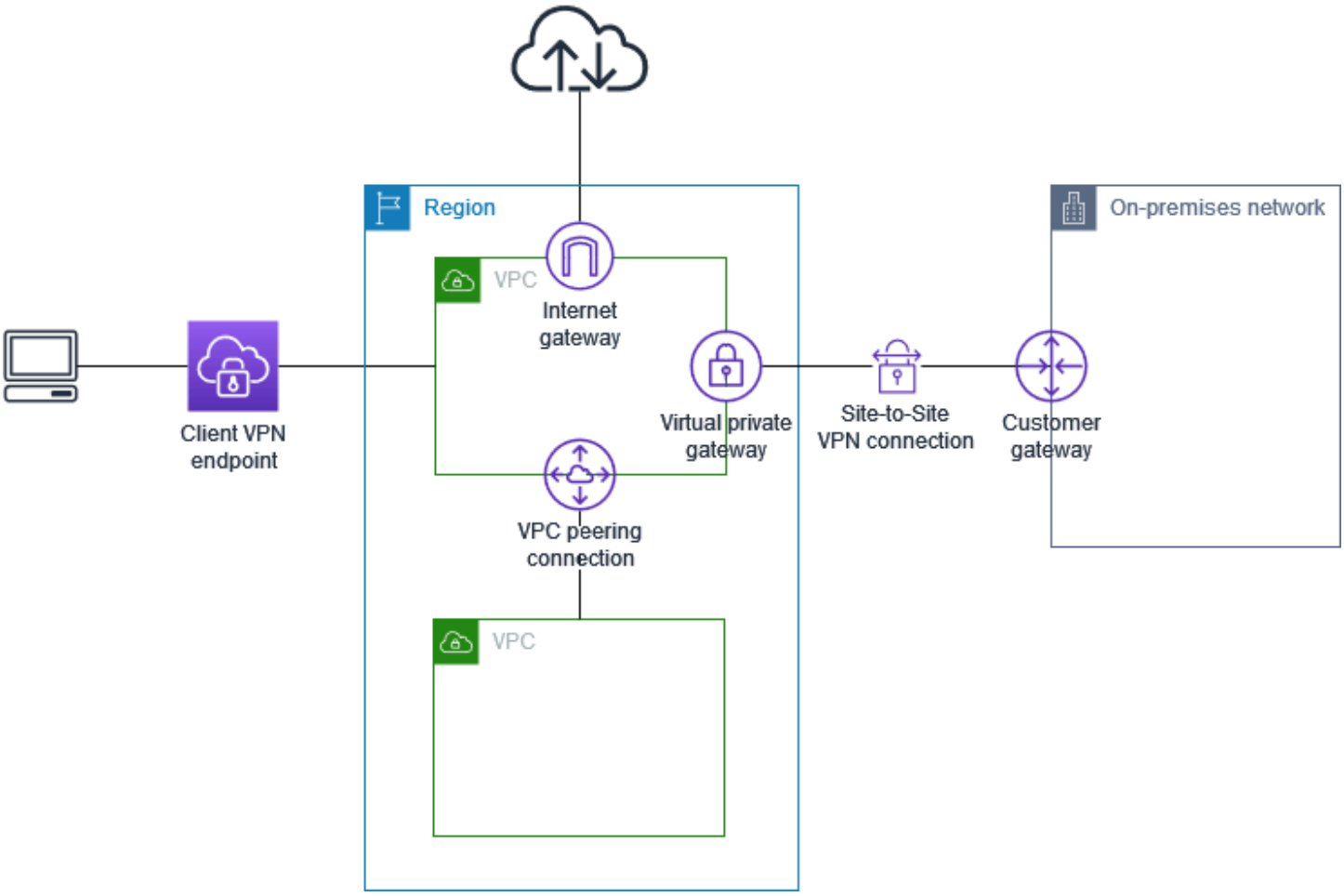
Como AWS Client VPN funciona

Com AWS Client VPN, há dois tipos de personas de usuário que interagem com o endpoint do Client VPN: administradores e clientes.

O administrador é responsável por criar e configurar o serviço. Isso envolve criar o endpoint da Client VPN, associar a rede de destino, configurar as regras de autorização e configurar rotas adicionais (se necessário). Depois que o endpoint da Client VPN é criado e configurado, o administrador faz download do arquivo de configuração do endpoint da Client VPN e o distribui aos clientes que precisam de acesso. O arquivo de configuração do endpoint da Client VPN inclui o nome DNS do endpoint da Client VPN e informações de autenticação necessárias para estabelecer uma sessão VPN. Para obter mais informações sobre a configuração do serviço, consulte Comece com AWS Client VPN.

O cliente é o usuário final. É a pessoa que se conecta ao endpoint da Client VPN para estabelecer uma sessão de VPN. O cliente estabelece a sessão de VPN em seu computador local ou dispositivo móvel usando uma aplicação cliente de VPN baseado no OpenVPN. Depois de estabelecer a sessão de VPN, ele pode acessar com segurança os recursos na VPC em que a sub-rede associada está localizada. Eles também podem acessar outros recursos em AWS uma rede local ou em outros clientes se as regras de rota e autorização necessárias tiverem sido configuradas. Para obter mais informações sobre como se conectar a um endpoint da Client VPN para estabelecer uma sessão de VPN, consulte Conceitos básicos no Guia do usuário do AWS Client VPN .

O gráfico a seguir ilustra a arquitetura básica da Client VPN.



Cenários e exemplos da Client VPN

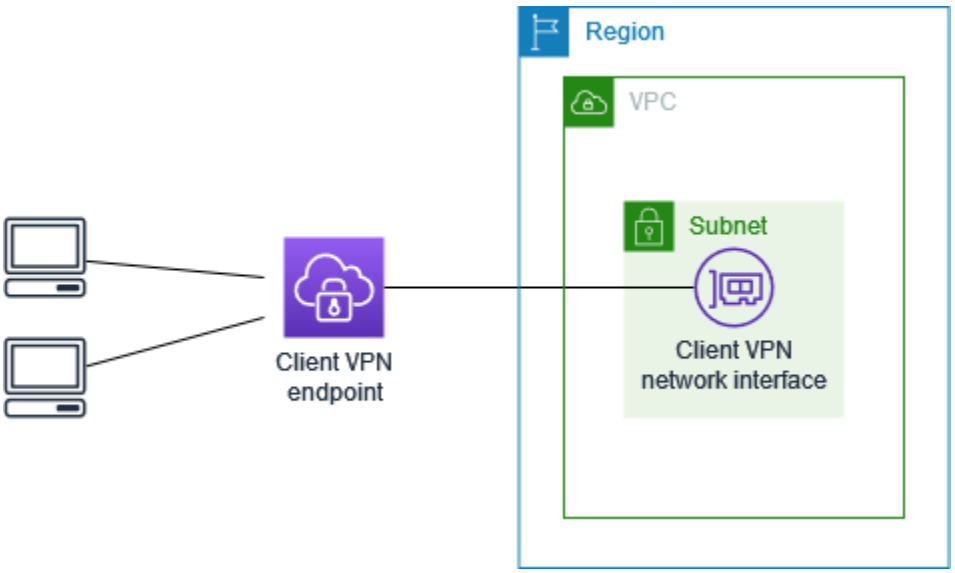
AWS Client VPN é uma solução VPN de acesso remoto totalmente gerenciada que você usa para permitir que os clientes tenham acesso seguro aos recursos tanto na rede local AWS quanto na sua. Há várias opções de como você configura o acesso. Esta seção fornece exemplos de como criar e configurar o acesso à Client VPN para seus clientes.

Cenários

- the section called “Acesso a uma VPC”
- the section called “Acesso a uma VPC emparelhada”
- the section called “Acesso a uma rede on-premises”
- the section called “Acesso à Internet”
- the section called “lient-to-clientAcesso C”
- the section called “Restringir o acesso à sua rede”

Acesso a uma VPC usando o Client VPN

A AWS Client VPN configuração desse cenário inclui uma única VPC de destino. Ela é recomendada quando você precisa permitir que os clientes tenham acesso aos recursos dentro de uma única VPC.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC a ser associada ao endpoint do Client VPN e anote IPv4 seus intervalos de CIDR.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints da Client VPN em Regras e práticas recomendadas para utilizar o AWS Client VPN.

Para implementar essa configuração

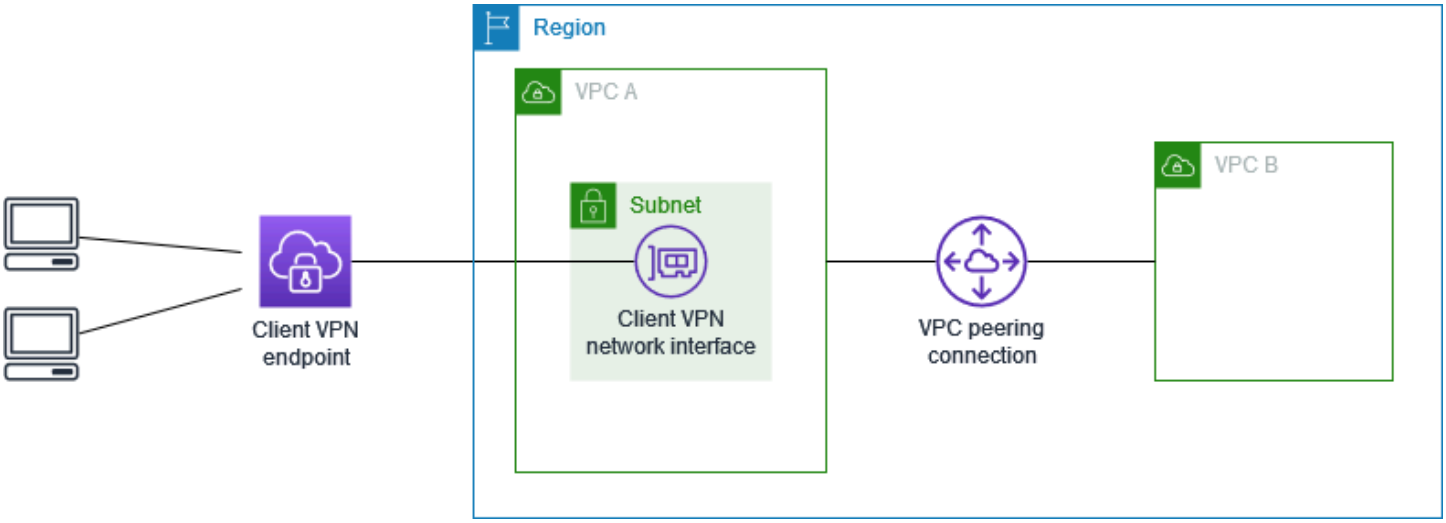
1. Crie um endpoint da Client VPN na mesma região que a VPC. Para fazer isso, execute as etapas descritas em Crie um AWS Client VPN endpoint.
2. Associe a sub-rede ao endpoint da Client VPN. Para fazer isso, execute as etapas descritas em Associar uma rede de destino a um endpoint do AWS Client VPN e selecione a sub-rede e a VPC que você identificou anteriormente.
3. Adicione uma regra de autorização para fornecer acesso à VPC para os clientes. Para fazer isso, execute as etapas descritas em eAdicionar uma regra de autorização, em Rede de destino, insira o intervalo IPv4 CIDR da VPC.

4. Adicione uma regra aos grupos de segurança dos recursos para permitir o tráfego do grupo de segurança que foi aplicado à associação de sub-rede na etapa 2. Para obter mais informações, consulte Grupos de segurança.

Acesso a uma VPC emparelhada usando o Client VPN

A AWS Client VPN configuração desse cenário inclui uma VPC de destino (VPC A) que é emparelhada com uma VPC adicional (VPC B). Recomendamos essa configuração se você precisar dar aos clientes acesso aos recursos dentro de uma VPC de destino e a outras VPCs que estejam emparelhadas com ela (como a VPC B).

> **Note**
>
> O procedimento para permitir o acesso a uma VPC com emparelhamento (descrito após o diagrama de rede) será necessário somente se o endpoint da Client VPN tiver sido configurado para o modo de túnel dividido. No modo de túnel inteiro, o acesso à VPC emparelhada é permitido por padrão.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC a ser associada ao endpoint do Client VPN e anote IPv4 seus intervalos de CIDR.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.

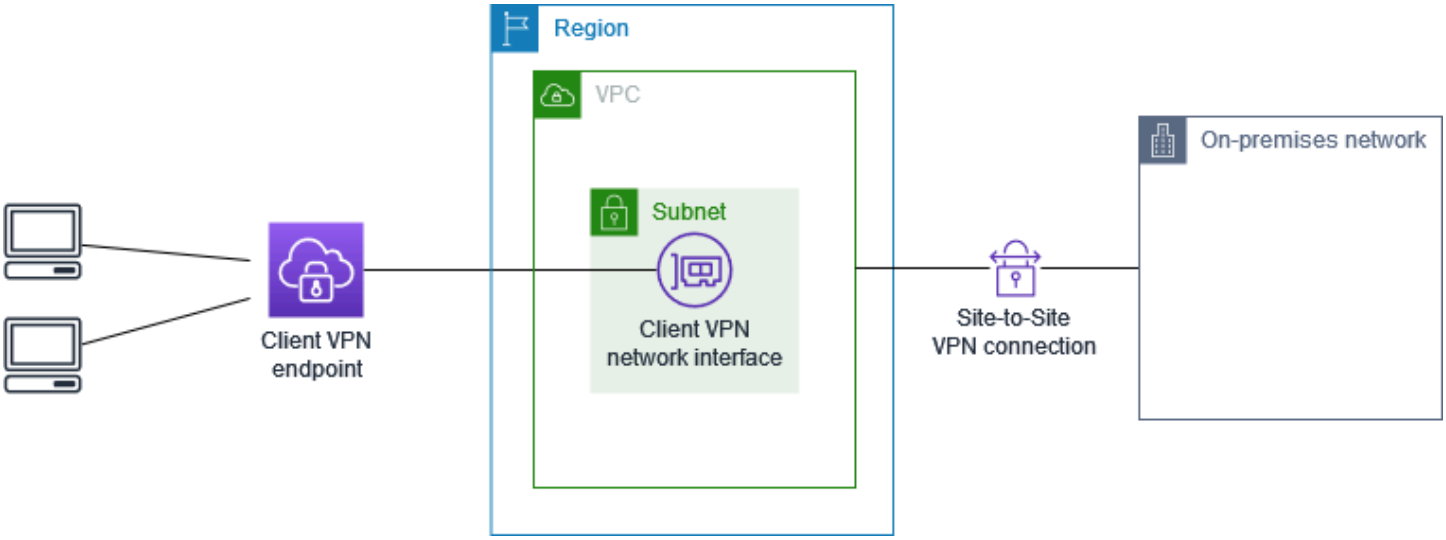
- Revise as regras e as limitações dos endpoints da Client VPN em Regras e práticas recomendadas para utilizar o AWS Client VPN.

Para implementar essa configuração

1. Estabeleça a conexão de emparelhamento de VPC entre o. VPCs Siga as etapas em Criar e aceitar uma conexão de emparelhamento de VPC no Guia de emparelhamento da Amazon VPC. Confirme se as instâncias na VPC A podem se comunicar com as instâncias na VPC B utilizando a conexão emparelhada.
2. Crie um endpoint da Client VPN na mesma região que a VPC de destino. No diagrama, essa é a VPC A. Para fazer isso, execute as etapas descritas em Crie um AWS Client VPN endpoint.
3. Associe a sub-rede identificada ao endpoint da Client VPN que você criou. Para fazer isso, execute as etapas descritas em Associar uma rede de destino a um endpoint do AWS Client VPN e selecione a sub-rede e a VPC. Por padrão, associamos o grupo de segurança padrão da VPC ao endpoint da Client VPN. É possível associar um grupo de segurança diferente utilizando as etapas descritas em the section called “Aplicar um grupo de segurança a uma rede de destino”.
4. Adicione uma regra de autorização para fornecer acesso à VPC de destino para os clientes. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização. Para ativar a rede de destino, insira o intervalo IPv4 CIDR da VPC.
5. Adicione uma rota para direcionar o tráfego à VPC emparelhada. No diagrama, essa é a VPC B. Para fazer isso, execute as etapas descritas em Crie uma rota AWS Client VPN de endpoint. Em Destino da rota, insira o intervalo IPv4 CIDR da VPC emparelhada. Em ID da sub-rede da VPC de destino, selecione a sub-rede associada ao endpoint da Client VPN.
6. Adicione uma regra de autorização para fornecer os acesso à VPC emparelhada para os clientes. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização. Em Rede de destino, insira o intervalo IPv4 CIDR da VPC emparelhada.
7. Adicione uma regra aos grupos de segurança de suas instâncias na VPC A e na VPC B para permitir o tráfego do grupo de segurança que foi aplicado ao endpoint da Client VPN na etapa 3. Para obter mais informações, consulte Grupos de segurança.

Acesso a uma rede on-premises que usa o Client VPN

A AWS Client VPN configuração desse cenário inclui acesso somente a uma rede local. Ela é recomendada quando você precisa permitir que os clientes tenham acesso aos recursos dentro de uma rede no local apenas.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC a ser associada ao endpoint do Client VPN e anote IPv4 seus intervalos de CIDR.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints da Client VPN em Regras e práticas recomendadas para utilizar o AWS Client VPN.

Para implementar essa configuração

1. Habilite a comunicação entre a VPC e sua própria rede local por meio de uma AWS Site-to-Site conexão VPN. Para fazer isso, execute as etapas descritas em Conceitos básicos no Guia do usuário do AWS Site-to-Site VPN .

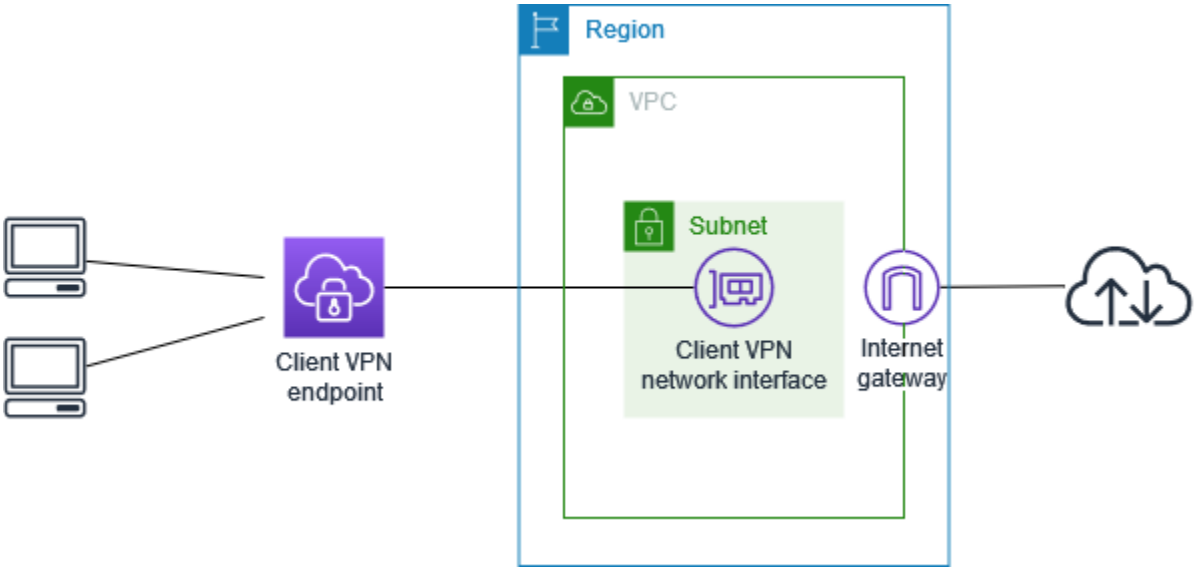
> **Note**
>
> Como alternativa, você pode implementar esse cenário usando uma AWS Direct Connect conexão entre sua VPC e sua rede local. Para obter mais informações, consulte o Guia do usuário do AWS Direct Connect.

2. Teste a conexão AWS Site-to-Site VPN que você criou na etapa anterior. Para fazer isso, execute as etapas descritas em Teste da conexão Site-to-Site VPN no Guia do AWS Site-to-Site VPN usuário. Se a conexão VPN estiver funcionando conforme o esperado, continue para a próxima etapa.
3. Crie um endpoint da Client VPN na mesma região que a VPC. Para fazer isso, execute as etapas descritas em Crie um AWS Client VPN endpoint.
4. Associe a sub-rede que você identificou anteriormente ao endpoint da Client VPN. Para fazer isso, execute as etapas descritas em Associar uma rede de destino a um endpoint do AWS Client VPN e selecione a VPC e a sub-rede.
5. Adicione uma rota que permita o acesso à conexão AWS Site-to-Site VPN. Para fazer isso, execute as etapas descritas emCrie uma rota AWS Client VPN de endpoint; em Destino da rota, insira o intervalo IPv4 CIDR da conexão AWS Site-to-Site VPN e, em Target VPC Subnet ID, selecione a sub-rede que você associou ao endpoint Client VPN.
6. Adicione uma regra de autorização para dar aos clientes acesso à conexão AWS Site-to-Site VPN. Para fazer isso, execute as etapas descritas emAdicionar uma regra de autorização a um endpoint do AWS Client VPN; para Rede de destino, insira o intervalo IPv4 CIDR da conexão AWS Site-to-Site VPN.

Acesso à internet usando o Client VPN

A AWS Client VPN configuração desse cenário inclui uma única VPC de destino e acesso à Internet. Ela é recomendada quando você precisa permitir que os clientes tenham acesso aos recursos dentro de uma única VPC de destino e também permitir o acesso à Internet.

Se você já concluiu o tutorial Comece com AWS Client VPN, então já implementou esse cenário.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC a ser associada ao endpoint do Client VPN e anote IPv4 seus intervalos de CIDR.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints da Client VPN em Regras e práticas recomendadas para utilizar o AWS Client VPN.

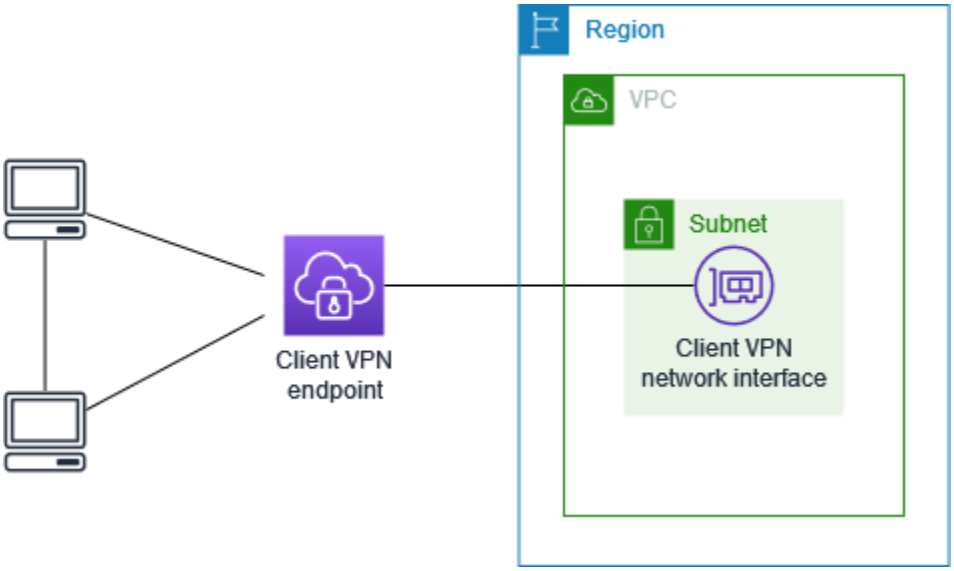
Para implementar essa configuração

1. Verifique se o grupo de segurança que você usará para o endpoint da VPN do cliente permite tráfego de saída para a Internet. Para fazer isso, adicione regras de saída que permitam tráfego HTTP e HTTPS para 0.0.0.0/0.
2. Crie um gateway de internet e anexe-o à sua VPC. Para obter mais informações, consulte Criar e anexar um gateway da Internet no Guia do usuário do Amazon VPC.
3. Torne a sub-rede pública, adicionando uma rota para o gateway de internet à sua tabela de rotas. No console da VPC, escolha Subnets (Sub-redes), selecione a sub-rede que você pretende associar ao endpoint da Client VPN, escolha Route Table (Tabela de rotas) e escolha o ID da tabela de rotas. Escolha Actions (Ações), Edit routes (Editar rotas) e depois Add route (Adicionar rota). Em Destination (Destino), insira `0.0.0.0/0` e, em Target (Destino), escolha o gateway de internet da etapa anterior.

4. Crie um endpoint da Client VPN na mesma região que a VPC. Para fazer isso, execute as etapas descritas em Crie um AWS Client VPN endpoint.
5. Associe a sub-rede que você identificou anteriormente ao endpoint da Client VPN. Para fazer isso, execute as etapas descritas em Associar uma rede de destino a um endpoint do AWS Client VPN e selecione a VPC e a sub-rede.
6. Adicione uma regra de autorização para fornecer acesso à VPC para os clientes. Para fazer isso, execute as etapas descritas emAdicionar uma regra de autorização; e para ativar a rede de destino, insira o intervalo IPv4 CIDR da VPC.
7. Adicione uma rota que permita tráfego para a Internet. Para fazer isso, execute as etapas descritas em Crie uma rota AWS Client VPN de endpoint. Em Route destination (Destino da rota), insira `0.0.0.0/0` e, em Target VPC Subnet ID (ID da sub-rede da VPC de destino), selecione a sub-rede que você associou ao endpoint da Client VPN.
8. Adicione uma regra de autorização para fornecer acesso à Internet para os clientes. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização. Em Destination network (Rede de destino), insira `0.0.0.0/0`.
9. Verifique se os grupos de segurança para os recursos em sua VPC têm uma regra que permita o acesso do grupo de segurança com o endpoint da VPN do cliente. Isso permite que os clientes acessem os recursos na VPC.

Client-to-client acesso usando Client VPN

A AWS Client VPN configuração desse cenário permite que os clientes acessem uma única VPC e roteiem o tráfego entre si. Recomendamos essa configuração se os clientes que se conectam ao mesmo endpoint da Client VPN também precisam se comunicar uns com os outros. Os clientes podem se comunicar entre si usando o endereço IP exclusivo atribuído a eles do intervalo CIDR do cliente quando se conectam ao endpoint da Client VPN.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC a ser associada ao endpoint do Client VPN e anote IPv4 seus intervalos de CIDR.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints da Client VPN em Regras e práticas recomendadas para utilizar o AWS Client VPN.

> **Note**
>
> Neste cenário, não há compatibilidade com regras de autorização baseadas em rede que utilizam grupos do Active Directory ou grupos IdP baseados em SAML.

Para implementar essa configuração

1. Crie um endpoint da Client VPN na mesma região que a VPC. Para fazer isso, execute as etapas descritas em Crie um AWS Client VPN endpoint.
2. Associe a sub-rede que você identificou anteriormente ao endpoint da Client VPN. Para fazer isso, execute as etapas descritas em Associar uma rede de destino a um endpoint do AWS Client VPN e selecione a VPC e a sub-rede.

3. Adicione uma rota à rede local na tabela de rotas. Para fazer isso, execute as etapas descritas em Crie uma rota AWS Client VPN de endpoint. Em Route destination (Destino da rota), insira o intervalo CIDR do cliente e, em Target VPC Subnet ID (ID de sub-rede da VPC de destino), especifique `local`.
4. Adicione uma regra de autorização para fornecer acesso à VPC para os clientes. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização. Para ativar a rede de destino, insira o intervalo IPv4 CIDR da VPC.
5. Adicione uma regra de autorização para conceder aos clientes acesso ao intervalo CIDR do cliente. Para fazer isso, execute as etapas descritas em Adicionar uma regra de autorização. Em Destination network to enable (Rede de destino para permitir acesso), insira o intervalo CIDR do cliente.

Restrição do acesso à rede usando o Client VPN

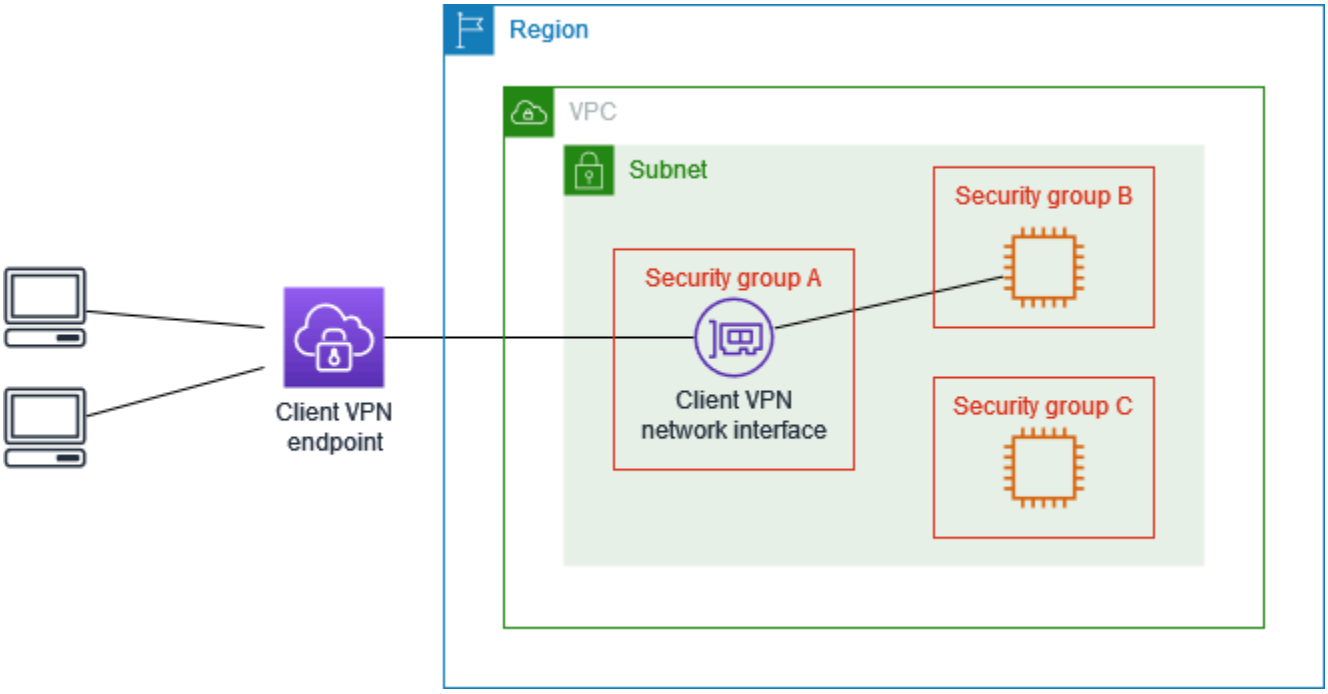
Você pode configurar seu AWS Client VPN endpoint para restringir o acesso a recursos específicos em sua VPC. Para autenticação baseada no usuário, você também pode restringir o acesso a partes da rede, com base no grupo de usuários que acessa o endpoint da Client VPN.

Restringir o acesso usando grupos de segurança

É possível conceder ou negar acesso a recursos específicos em sua VPC adicionando ou removendo regras de grupo de segurança que fazem referência ao grupo de segurança que foi aplicado à associação da rede de destino (o grupo de segurança da Client VPN). Essa configuração é comentada no cenário descrito em Acesso a uma VPC usando o Client VPN. Ela é aplicada além da regra de autorização configurada naquele cenário.

Para conceder acesso a um recurso específico, identifique o grupo de segurança associado à instância em que o recurso está sendo executado. Crie uma regra que permita o tráfego do grupo de segurança da Client VPN.

No diagrama a seguir, o grupo de segurança A é o grupo de segurança Client VPN, o grupo de segurança B está associado a uma EC2 instância e o grupo de segurança C está associado a uma EC2 instância. Se você adicionar uma regra ao grupo de segurança B que permita o acesso do grupo de segurança A, os clientes poderão acessar a instância associada ao grupo de segurança B. Se o grupo de segurança C não tiver uma regra que permita o acesso do grupo de segurança A, os clientes não poderão acessar a instância associada ao grupo de segurança C.



Antes de começar, verifique se o grupo de segurança da Client VPN está associado a outros recursos em sua VPC. Se você adicionar ou remover regras que fazem referência ao grupo de segurança da Client VPN, poderá conceder ou negar acesso aos outros recursos associados também. Para evitar isso, use um grupo de segurança criado especificamente para uso com seu endpoint da Client VPN.

Como criar uma regra de grupo de segurança

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Security Groups (Grupos de segurança).
3. Escolha o grupo de segurança associado à instância em que o recurso está sendo executado.
4. Escolha Actions (Ações), Edit inbound rules (Editar regras de entrada).
5. Selecione Add Rule (Adicionar regra) e faça o seguinte:
   - Em Type (Tipo), escolha All traffic (Todo o tráfego), ou um tipo específico de tráfego que você deseja permitir.
   - Para Source (Origem), escolha Custom (Personalizar) e insira ou escolha o ID do grupo de segurança da Client VPN.
6. Selecione Save rules (Salvar regras).

Para remover o acesso a um recurso específico, verifique o grupo de segurança associado à instância em que o recurso está sendo executado. Se houver uma regra que permita o tráfego do grupo de segurança da Client VPN, exclua-a.

Como verificar as regras do grupo de segurança

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Security Groups (Grupos de segurança).
3. Escolha Inbound Rules (Regras de entrada).
4. Revise a lista de regras. Se houver uma regra em que Source (Origem) seja o grupo de segurança da Client VPN, escolha Edit rules (Editar Regras) e selecione Delete (Excluir) (o ícone x) para a regra. Selecione Salvar rules.

Restringir o acesso com base em grupos de usuários

Se o endpoint da Client VPN estiver configurado para autenticação baseada no usuário, você poderá conceder a grupos específicos de usuários acesso a partes específicas da rede. Para fazer isso, conclua as seguintes etapas:

1. Configure usuários e grupos em AWS Directory Service ou em seu IdP. Para obter mais informações, consulte os tópicos a seguir.
   - Autenticação do Active Directory na Client VPN
   - Requisitos e considerações para autenticação federada baseada em SAML
2. Crie uma regra de autorização para seu endpoint da Client VPN que permita a um grupo especificado acesso a toda a rede ou parte dela. Para obter mais informações, consulte AWS Client VPN regras de autorização.

Se o endpoint da Client VPN estiver configurado para autenticação mútua, você não poderá configurar grupos de usuários. Ao criar uma regra de autorização, você deve conceder acesso a todos os usuários. Para permitir que grupos específicos de usuários acessem partes específicas da rede, é possível criar vários endpoints da Client VPN. Por exemplo, para cada grupo de usuários que acessa sua rede, faça o seguinte:

1. Crie um conjunto de certificados e chaves de servidor e cliente para esse grupo de usuários. Para obter mais informações, consulte Autenticação mútua em AWS Client VPN.

2. Crie um endpoint da Client VPN. Para obter mais informações, consulte Crie um AWS Client VPN endpoint.
3. Crie uma regra de autorização que conceda acesso a toda a rede ou parte dela. Por exemplo, para um endpoint da Client VPN usado por administradores, você pode criar uma regra de autorização que conceda acesso a toda a rede. Para obter mais informações, consulte Adicionar uma regra de autorização.

Autenticação do cliente em AWS Client VPN

A autenticação do cliente é implementada no primeiro ponto de entrada na AWS nuvem. Ela é usada para determinar se os clientes têm permissão para se conectar ao endpoint da Client VPN. Se a autenticação for bem-sucedida, os clientes se conectarão ao endpoint da cliente VPN e estabelecerão uma sessão de VPN. Se a autenticação falhar, a conexão será negada, e o cliente será impedido de estabelecer uma sessão de VPN.

O VPN do Cliente oferece os seguintes tipos de autenticação de cliente:

- Autenticação do Active Directory (baseada no usuário)
- Autenticação mútua (baseada em certificado)
- Single Sign-On (autenticação federada baseada em SAML) (baseado no usuário)

É possível usar apenas um dos métodos anteriores ou uma combinação de autenticação mútua com um método baseado em usuário, como o seguinte:

- Autenticação mútua e autenticação federada
- Autenticação mútua e autenticação do Active Directory

> **Important**
>
> - Para criar um endpoint da Client VPN, você deve provisionar um certificado de servidor no AWS Certificate Manager, independentemente do tipo de autenticação usado. Para obter mais informações sobre como criar e provisionar um certificado de servidor, consulte as etapas em Autenticação mútua em AWS Client VPN.

- Se você usar uma combinação de autenticação mútua e autenticação baseada em usuário, os dois métodos devem ser usados para se autenticar corretamente na VPN.

Autenticação do Active Directory na Client VPN

O Client VPN fornece suporte ao Active Directory por meio da integração com o. AWS Directory Service Com a autenticação via Active Directory, os clientes são autenticados com grupos existentes do Active Directory. Usando AWS Directory Service, o Client VPN pode se conectar aos Active Directories existentes provisionados em AWS ou em sua rede local. Isso permite que você use sua infraestrutura de autenticação de cliente existente. Se você estiver usando um Active Directory local e não tiver um Microsoft AD AWS gerenciado existente, deverá configurar um conector do Active Directory (AD Connector). É possível usar um servidor do Active Directory para autenticar os usuários. Para obter mais informações sobre a integração do Active Directory, consulte o Guia de administração do AWS Directory Service.

A cliente VPN é compatível com a autenticação multifator (MFA) quando ela está habilitada para o Managed Microsoft AD da AWS ou o AD Connector. Se a MFA estiver habilitada, os clientes devem inserir um nome de usuário, senha e código MFA ao se conectarem a um endpoint do cliente VPN. Para obter mais informações sobre como habilitar a MFA, consulte Habilitar a autenticação multifator para o Managed Microsoft AD da AWS e Habilitar a autenticação multifator para o AD Connector no Guia de administração do AWS Directory Service .

Para obter cotas e regras para configurar usuários e grupos no Active Directory, consulte Cotas de usuários e grupos.

Autenticação mútua em AWS Client VPN

Com a autenticação mútua, a Client VPN usa certificados para realizar a autenticação entre o cliente e o servidor. Os certificados são uma forma digital de identificação emitida por uma autoridade certificadora (CA). O servidor usa certificados de cliente para autenticar clientes quando eles tentam se conectar ao endpoint do cliente VPN. É necessário criar um certificado e uma chave de servidor e pelo menos um certificado e uma chave de cliente.

Você deve carregar o certificado do servidor para AWS Certificate Manager (ACM) e especificá-lo ao criar um endpoint Client VPN. Ao fazer upload do certificado do servidor no ACM, você também especifica a autoridade de certificação (CA). Você precisa fazer upload do certificado de cliente no

ACM somente quando a CA do certificado de cliente for diferente da CA do certificado de servidor. Para obter mais informações sobre o ACM, consulte o Guia do usuário do AWS Certificate Manager.

É possível criar um certificado de cliente separado e uma chave para cada cliente que se conectará ao endpoint do cliente VPN. Isso permite revogar um certificado de cliente específico se um usuário sair de sua organização. Nesse caso, ao criar o endpoint da Client VPN, é possível especificar o ARN de certificado de servidor para o certificado de cliente, desde que o certificado de cliente seja emitido pela mesma CA que o certificado de servidor.

Os certificados usados no AWS Client VPN devem seguir a RFC 5280: Certificado de infraestrutura de chave pública X.509 da Internet e perfil da lista de revogação de certificados (CRL), incluindo as extensões de certificado especificadas na seção 4.2 do memorando.

> **Note**
>
> Um endpoint do cliente VPN é compatível apenas com tamanhos de chave RSA de 1024 bits e 2048 bits. Além disso, o certificado do cliente deve ter o atributo CN no campo Subject (Assunto).
>
> Quando os certificados usados com o serviço Client VPN são atualizados, seja por meio da rotação automática do ACM, da importação manual de um novo certificado ou de atualizações de metadados no IAM Identity Center, o serviço Client VPN atualizará automaticamente o endpoint do Client VPN com o certificado mais recente. Esse é um processo automatizado que pode levar até 5 horas.

Tarefas

- Habilite a autenticação mútua para AWS Client VPN
- Renove seu certificado de servidor para AWS Client VPN

Habilite a autenticação mútua para AWS Client VPN

É possível ativar a autenticação mútua na Client VPN no Linux/MacOS ou no Windows.

Linux/macOS

O procedimento a seguir usa o OpenVPN easy-rsa para gerar os certificados e as chaves de servidor e cliente e faz upload do certificado e da chave de servidor no ACM. Para obter mais informações, consulte a seção LER de início rápido do Easy-RSA 3.

Para gerar os certificados e as chaves de servidor e cliente e transferi-los por upload ao ACM

1. Clone o repositório easy-rsa do OpenVPN para o computador local e navegue até a pasta `easy-rsa/easyrsa3`.

   ```
   $ git clone https://github.com/OpenVPN/easy-rsa.git
   ```

   ```
   $ cd easy-rsa/easyrsa3
   ```

2. Inicialize um novo ambiente PKI.

   ```
   $ ./easyrsa init-pki
   ```

3. Para criar uma nova autoridade de certificação (CA), execute este comando e siga as instruções.

   ```
   $ ./easyrsa build-ca nopass
   ```

4. Gere o certificado e a chave de servidor.

   ```
   $ ./easyrsa --san=DNS:server build-server-full server nopass
   ```

5. Gere o certificado e a chave de cliente.

   Certifique-se de salvar o certificado de cliente e a chave privada de cliente, pois você precisará deles ao configurar o cliente.

   ```
   $ ./easyrsa build-client-full client1.domain.tld nopass
   ```

   Opcionalmente, você pode repetir essa etapa para cada cliente (usuário final) que exija um certificado e uma chave de cliente.

6. Copie os certificados e as chaves de servidor e de cliente para uma pasta personalizada e depois navegue até ela.

   Antes de copiar os certificados e as chaves, crie a pasta personalizada usando o comando `mkdir`. O exemplo a seguir cria uma pasta personalizada em seu diretório base.

   ```
   $ mkdir ~/custom_folder/
   $ cp pki/ca.crt ~/custom_folder/
   ```

```
$ cp pki/issued/server.crt ~/custom_folder/
$ cp pki/private/server.key ~/custom_folder/
$ cp pki/issued/client1.domain.tld.crt ~/custom_folder
$ cp pki/private/client1.domain.tld.key ~/custom_folder/
$ cd ~/custom_folder/
```

7. Faça upload do certificado e da chave do servidor e do certificado e da chave do cliente no ACM. Certifique-se de fazer upload deles na mesma região em que pretende criar o endpoint da Client VPN. Os comandos a seguir usam a AWS CLI para fazer upload dos certificados. Para fazer upload dos certificados usando o console do ACM, consulte Importar certificados no Guia do usuário do AWS Certificate Manager .

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

```
$ aws acm import-certificate --certificate fileb://client1.domain.tld.crt --
private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

Você não precisa necessariamente carregar o certificado do cliente no ACM. Se os certificados de servidor e de cliente tiverem sido emitidos pela mesma autoridade de certificação (CA), você poderá usar o ARN de certificado de servidor tanto para o servidor quanto para o cliente ao criar o endpoint do cliente VPN. Nas etapas acima, a mesma CA foi usada para criar ambos os certificados. Entretanto, as etapas para carregar o certificado do cliente estão incluídas para que as instruções fiquem completas.

Windows

O procedimento a seguir instala o software Easy-RSA 3.x e o usa para gerar os certificados e chaves do servidor e do cliente.

Para gerar os certificados e as chaves de servidor e cliente e carregá-los no ACM

1. Acesse a página de lançamentos do EasyRSA, baixe o arquivo ZIP para sua versão do Windows e extraia-o.
2. Abra um prompt de comando e navegue até o local para o qual a pasta `EasyRSA-3.x` foi extraída.
3. Execute o comando a seguir para abrir o shell do EasyRSA 3.

```
C:\Program Files\EasyRSA-3.x> .\EasyRSA-Start.bat
```

4. Inicialize um novo ambiente PKI.

```
# ./easyrsa init-pki
```

5. Para criar uma nova autoridade de certificação (CA), execute este comando e siga as instruções.

```
# ./easyrsa build-ca nopass
```

6. Gere o certificado e a chave de servidor.

```
# ./easyrsa --san=DNS:server build-server-full server nopass
```

7. Gere o certificado e a chave de cliente.

```
# ./easyrsa build-client-full client1.domain.tld nopass
```

   Opcionalmente, você pode repetir essa etapa para cada cliente (usuário final) que exija um certificado e uma chave de cliente.

8. Saia do shell do EasyRSA 3.

```
# exit
```

9. Copie os certificados e as chaves de servidor e de cliente para uma pasta personalizada e depois navegue até ela.

   Antes de copiar os certificados e as chaves, crie a pasta personalizada usando o comando `mkdir`. O exemplo a seguir cria uma pasta personalizada na unidade C:\.

```
C:\Program Files\EasyRSA-3.x> mkdir C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\ca.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\server.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\server.key C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\client1.domain.tld.crt C:
\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\client1.domain.tld.key C:
\custom_folder
```

```
C:\Program Files\EasyRSA-3.x> cd C:\custom_folder
```

10. Faça upload do certificado e da chave do servidor e do certificado e da chave do cliente no ACM. Certifique-se de fazer upload deles na mesma região em que pretende criar o endpoint da Client VPN. Os comandos a seguir usam o AWS CLI para carregar os certificados. Para fazer upload dos certificados usando o console do ACM, consulte Importar certificados no Guia do usuário do AWS Certificate Manager .

```
aws acm import-certificate \
    --certificate fileb://server.crt \
    --private-key fileb://server.key \
    --certificate-chain fileb://ca.crt
```

```
aws acm import-certificate \
    --certificate fileb://client1.domain.tld.crt \
    --private-key fileb://client1.domain.tld.key \
    --certificate-chain fileb://ca.crt
```

Você não precisa necessariamente carregar o certificado do cliente no ACM. Se os certificados de servidor e de cliente tiverem sido emitidos pela mesma autoridade de certificação (CA), você poderá usar o ARN de certificado de servidor tanto para o servidor quanto para o cliente ao criar o endpoint do cliente VPN. Nas etapas acima, a mesma CA foi usada para criar ambos os certificados. Entretanto, as etapas para carregar o certificado do cliente estão incluídas para que as instruções fiquem completas.

Renove seu certificado de servidor para AWS Client VPN

É possível utilizar o certificado do servidor VPN do Client que tenha expirado. Dependendo da versão do OpenVPN easy-rsa que você está utilizando, o processo irá variar. Consulte a documentação de renovação e revogação de certificados do Easy-RSA 3 para obter mais detalhes.

Para renovar o certificado de servidor

1. Execute um destes procedimentos:
   - Easy-RSA versão 3.1.x
     - Execute o comando de renovação do certificado.

```
$ ./easyrsa renew server nopass
```

- Easy-RSA versão 3.2.x

  a. Execute o comando expire.

  ```
  $ ./easyrsa expire server
  ```

  b. Assine um novo certificado.

  ```
  $ ./easyrsa --san=DNS:server sign-req server server
  ```

2. Crie uma pasta personalizada, copie os novos arquivos para ela e navegue até a pasta.

```
$ mkdir ~/custom_folder2
$ cp pki/ca.crt ~/custom_folder2/
$ cp pki/issued/server.crt ~/custom_folder2/
$ cp pki/private/server.key ~/custom_folder2/
$ cd ~/custom_folder2/
```

3. Importe os novos arquivos para o ACM. É necessário importá-los na mesma região que o endpoint da Client VPN.

```
$ aws acm import-certificate \
    --certificate fileb://server.crt \
    --private-key fileb://server.key \
    --certificate-chain fileb://ca.crt \
    --certificate-arn
 arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-12345678901
```

Single Sign-On — Autenticação federada baseada em SAML 2.0 — na Client VPN

AWS Client VPN oferece suporte à federação de identidades com o Security Assertion Markup Language 2.0 (SAML 2.0) para endpoints Client VPN. Você pode usar provedores de identidade (IdPs) que oferecem suporte ao SAML 2.0 para criar identidades de usuário centralizadas. Depois, você pode configurar um endpoint do cliente VPN para usar a autenticação federada baseada

em SAML e associá-lo ao IdP. Os usuários se conectam ao endpoint do cliente VPN usando as respectivas credenciais centralizadas.

Tópicos

- Habilitar SAML para AWS Client VPN
- Fluxo de trabalho de autenticação
- Requisitos e considerações para autenticação federada baseada em SAML
- Recursos de configuração de IdPs baseados em SAML

Habilitar SAML para AWS Client VPN

É possível habilitar o SAML para login único para Client VPN ao seguir estas etapas. Como alternativa, se você tiver habilitado o portal de autoatendimento para o endpoint da cliente VPN, instrua os usuários a acessá-lo para obter o arquivo de configuração e o cliente fornecido pela AWS . Para obter mais informações, consulte AWS Client VPN acesso ao portal de autoatendimento.

Para permitir que o IdP baseado em SAML funcione com um endpoint da Client VPN, você deve fazer o seguinte.

1. Crie um aplicativo baseado em SAML no IdP escolhido para usar com AWS Client VPN ou use um aplicativo existente.
2. Configure seu IdP para estabelecer uma relação de confiança com a AWS. Para obter recursos, consulte Recursos de configuração de IdPs baseados em SAML.
3. No IdP, gere e faça download de um documento de metadados de federação que descreve sua organização como um IdP.

   Esse documento XML assinado é usado para estabelecer a relação de confiança entre a AWS e o IdP.
4. Crie um provedor de identidade SAML do IAM na mesma AWS conta do endpoint do Client VPN.

   O provedor de identidade SAML do IAM define a relação de confiança entre o IdP e AWS a confiança da sua organização usando o documento de metadados gerado pelo IdP. Para obter mais informações, consulte Criar provedores de identidade SAML do IAM no Guia do usuário do IAM. Se você atualizar posteriormente a configuração da aplicação no IdP, gere um novo documento de metadados e atualize seu provedor de identidade SAML do IAM.

> **Note**
>
> Não é necessário criar uma função do IAM para usar o provedor de identidade SAML do IAM.

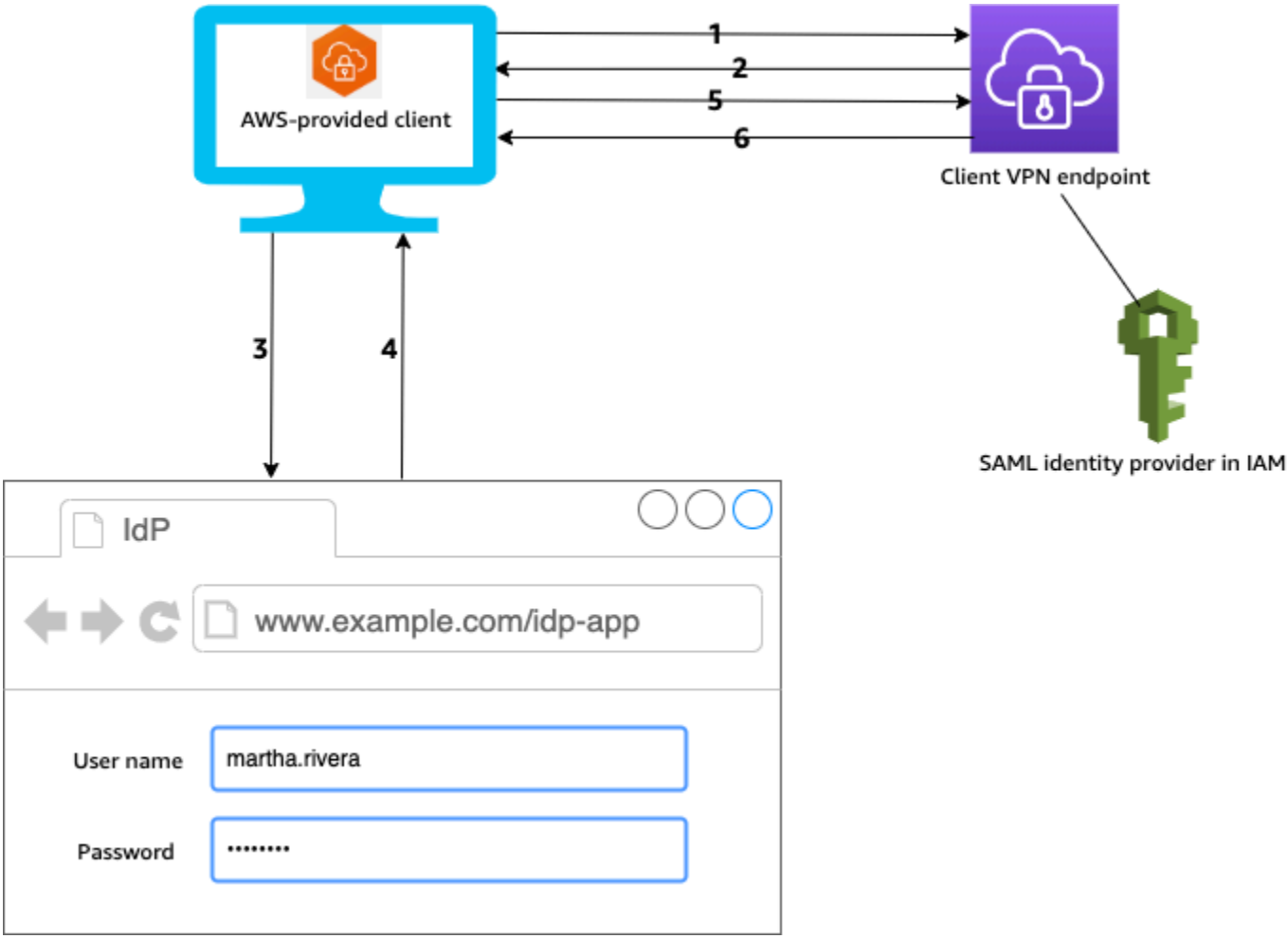
5. Crie um endpoint do cliente VPN.

   Especifique a autenticação federada como o tipo de autenticação e especifique o provedor de identidade SAML do IAM que você criou. Para obter mais informações, consulte Crie um AWS Client VPN endpoint.

6. Exporte o arquivo de configuração do cliente e distribua-o aos usuários. Instrua os usuários a fazerem download da versão mais recente do cliente fornecido pela AWS e usá-la para carregar o arquivo de configuração e se conectar ao endpoint da cliente VPN.

Fluxo de trabalho de autenticação

O diagrama a seguir fornece uma visão geral do fluxo de trabalho de autenticação para um endpoint do cliente VPN que usa autenticação federada baseada em SAML. Ao criar e configurar o endpoint do cliente VPN, você especifica o provedor de identidade SAML do IAM.



1. O usuário abre o cliente AWS fornecido em seu dispositivo e inicia uma conexão com o endpoint do Client VPN.
2. O endpoint do cliente VPN envia um URL de IdP e uma solicitação de autenticação de volta ao cliente, com base nas informações fornecidas no provedor de identidade SAML do IAM.
3. O cliente AWS fornecido abre uma nova janela do navegador no dispositivo do usuário. O navegador faz uma solicitação para o IdP e exibe uma página de login.
4. O usuário insere as credenciais na página de login e o IdP envia uma declaração SAML assinada de volta ao cliente.
5. O cliente AWS fornecido envia a declaração SAML para o endpoint do Client VPN.
6. O endpoint do cliente VPN valida a declaração e permite ou nega o acesso ao usuário.

Requisitos e considerações para autenticação federada baseada em SAML

Veja a seguir requisitos e considerações para autenticação federada baseada em SAML.

- Para obter cotas e regras para configurar usuários e grupos em um IdP baseado em SAML, consulte Cotas de usuários e grupos.
- A declaração SAML e os documentos SAML devem ser assinados.
- AWS Client VPN só oferece suporte às condições AudienceRestriction "" e "NotBefore e NotOnOrAfter" nas afirmações do SAML.
- O tamanho máximo compatível com respostas SAML é 128 KB.
- AWS Client VPN não fornece solicitações de autenticação assinadas.
- Não há compatibilidade com logout único SAML. Os usuários podem sair desconectando-se do cliente AWS fornecido ou você pode encerrar as conexões.
- Um endpoint do cliente VPN é compatível apenas com um único IdP.
- A autenticação multifator (MFA) é permitida quando está habilitada no IdP.
- Os usuários devem usar o cliente AWS fornecido para se conectar ao endpoint do Client VPN. Eles devem usar a versão 1.2.0 ou posterior. Para obter mais informações, consulte Conectar usando o cliente AWS fornecido.
- Os seguintes navegadores são compatíveis com a autenticação IdP: Apple Safari, Google Chrome, Microsoft Edge e Mozilla Firefox.
- O cliente AWS fornecido reserva a porta TCP 35001 nos dispositivos dos usuários para a resposta SAML.
- Se o documento de metadados do provedor de identidade SAML do IAM for atualizado com um URL incorreto ou mal-intencionado, isso poderá causar problemas de autenticação para os usuários ou resultar em ataques de phishing. Portanto, recomendamos que você use o AWS CloudTrail para monitorar atualizações feitas no provedor de identidade SAML do IAM. Para obter mais informações, consulte Como registrar o IAM e chamadas do AWS STS com o AWS CloudTrail no Guia do usuário do IAM.
- AWS Client VPN envia uma solicitação AuthN ao IdP por meio de uma associação de redirecionamento HTTP. Portanto, o IdP deve ser compatível com a vinculação de redirecionamento HTTP e deve estar presente no documento de metadados do IdP.
- Para a declaração SAML, é preciso usar um formato de endereço de e-mail para o atributo `NameID`.
- Quando os certificados usados com o serviço Client VPN são atualizados, seja por meio da rotação automática do ACM, da importação manual de um novo certificado ou de atualizações de metadados no IAM Identity Center, o serviço Client VPN atualizará automaticamente o endpoint do Client VPN com o certificado mais recente. Esse é um processo automatizado que pode levar até 5 horas.

Recursos de configuração de IdPs baseados em SAML

A tabela a seguir lista o baseado em SAML com o IdPs qual testamos para uso e os recursos que podem ajudá-lo a configurar o IdP. AWS Client VPN

IdP	Recurso
Okta	Autenticar AWS Client VPN usuários com SAML
Microsoft Entra ID (antigo Azure Active Directory)	Para obter mais informações, consulte o Tutorial: Microsoft Entra na integração de login único (SSO) com o AWS ClientVPN no site de documentação da Microsoft.
JumpCloud	Integre com AWS Client VPN
AWS IAM Identity Center	Usando o IAM Identity Center com AWS Client VPN para autenticação e autorização

Informações do provedor de serviços para criar um aplicativo

Para criar um aplicativo baseado em SAML usando um IdP que não esteja listado na tabela anterior, use as informações a seguir para configurar as informações do provedor de serviços. AWS Client VPN

- URL do Assertion Consumer Service (ACS): `http://127.0.0.1:35001`
- URI do público: `urn:amazon:webservices:clientvpn`

Pelo menos um atributo deve ser incluído na resposta SAML do IdP. Veja os exemplos de atributo a seguir.

Atributo	Descrição
`FirstName`	O nome do usuário.
`LastName`	O sobrenome do usuário.

Atributo	Descrição
`memberOf`	Os grupos aos quais o usuário pertence.

> **Note**
>
> O atributo `memberOf` é necessário para usar as regras de autorização baseadas em grupos do Active Directory ou do IdP SAML. Também diferencia letras maiúsculas de minúsculas e deve ser configurado exatamente como especificado. Consulte Autorização com base em rede e AWS Client VPN regras de autorização para obter mais informações.

Suporte para o portal de autoatendimento

Se você habilitar o portal de autoatendimento do endpoint do cliente VPN, os usuários fazem login no portal usando as credenciais IdP baseadas em SAML.

Se o seu IdP oferecer suporte a vários Assertion Consumer Service (ACS) URLs, adicione o seguinte URL do ACS ao seu aplicativo.

```
https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

Se você estiver usando o endpoint do Client VPN em uma GovCloud região, use o seguinte URL do ACS em vez disso. Se você usar o mesmo aplicativo IDP para autenticar tanto para o padrão quanto para as GovCloud regiões, poderá adicionar os dois. URLs

```
https://gov.self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

Se o seu IdP não suportar vários ACS URLs, faça o seguinte:

1. Crie uma aplicação adicional baseado em SAML no IdP e especifique o seguinte URL do ACS.

   ```
   https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
   ```

2. Gere e faça download de um documento de metadados de federação.
3. Crie um provedor de identidade SAML do IAM na mesma AWS conta do endpoint do Client VPN. Para obter mais informações, consulte Criar provedores de identidade SAML do IAM no Guia do usuário do IAM.

> **Note**
>
> Crie este provedor de identidade SAML além daquele criado para a aplicação principal.

4. Crie o endpoint do cliente VPN e especifique os provedores de identidade SAML do IAM.

Autorização do cliente em AWS Client VPN

A VPN do cliente é compatível com dois tipos de autorização do cliente: grupos de segurança e autorização com base na rede (usando regras de autorização).

Grupos de segurança

Ao criar um terminal do VPN do Cliente, você pode especificar os grupos de segurança de uma VPC específica a serem aplicados ao terminal do VPN do Cliente. Quando você associa uma sub-rede a um terminal do VPN do Cliente, aplicamos automaticamente o grupo de segurança padrão da VPC. É possível alterar os grupos de segurança depois de criar o terminal do VPN do Cliente. Para obter mais informações, consulte Aplicar um grupo de segurança a uma rede de destino no AWS Client VPN. Os grupos de segurança estão associados às interfaces de rede do VPN do Cliente.

É possível permitir que os usuários do VPN do Cliente acessem suas aplicações em uma VPC adicionando uma regra aos grupos de segurança para permitir o tráfego do grupo de segurança que foi aplicado à associação.

Por outro lado, é possível restringir o acesso para usuários do VPN do Cliente não especificando o grupo de segurança que foi aplicado à associação ou removendo a regra que faz referência ao grupo de segurança de terminal do VPN do Cliente. As regras de grupo de segurança necessárias podem depender do tipo de acesso VPN a ser configurado. Para obter mais informações, consulte Cenários e exemplos da Client VPN.

Para obter mais informações sobre grupos de segurança de VPC, consulte Grupos de segurança para a VPC no Guia do usuário da Amazon VPC.

Autorização com base em rede

A autorização com base em rede é implementada com o uso de regras de autorização. Para cada rede à qual você deseja habilitar o acesso, é necessário configurar regras de autorização que limitam

os usuários que têm acesso. Para uma rede especificada, configure o grupo do Active Directory ou o grupo do IdP baseado em SAML que tem permissão de acesso. Somente os usuários que pertencerem ao grupo especificado poderão acessar a rede especificada. Se não estiver usando a autenticação federada baseada em Active Directory ou SAML, ou se quiser abrir o acesso a todos os usuários, você poderá especificar uma regra que conceda acesso a todos os clientes. Para obter mais informações, consulte AWS Client VPN regras de autorização.

Tarefas

- Crie uma regra de grupo AWS Client VPN de segurança de endpoint

Crie uma regra de grupo AWS Client VPN de segurança de endpoint

O grupo de segurança padrão da VPC aplicado ao associar uma sub-rede a um Client VPN pode restringir o tráfego do grupo de segurança padrão que você deseja permitir e, ao mesmo tempo, permitir tráfego indesejado. Utilize as etapas a seguir para criar uma regra de grupo de segurança de endpoint da Client VPN que permita ou restrinja o tráfego para um grupo de segurança de endpoint associado a um recurso ou uma aplicação. Para obter mais informações sobre regras de grupos de segurança, consulte Grupos de segurança para sua VPC no Guia do usuário da Amazon VPC.

Como adicionar uma regra que permita o tráfego do grupo de segurança do terminal do VPN do Cliente

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Security Groups (Grupos de segurança).
3. Escolha o grupo de segurança associado ao seu recurso ou aplicação e escolha Ações, Editar regras de entrada.
4. Escolha Adicionar regra.
5. Para Tipo, escolha Todo o tráfego. Como alternativa, é possível restringir o acesso a um tipo específico de tráfego, por exemplo, SSH.

   Em Origem, especifique o ID do grupo de segurança associado à rede de destino (sub-rede) do terminal do VPN do Cliente.
6. Escolha Salvar regras.

Autorização de conexão em AWS Client VPN

É possível configurar um manipulador de conexão de cliente para o endpoint da cliente VPN. O manipulador permite executar a lógica que autoriza uma nova conexão, baseada em atributos de dispositivo, usuário e conexão. O manipulador de conexão do cliente é executado depois que o serviço do VPN do cliente autenticou o dispositivo e o usuário.

Para configurar um manipulador de conexão do cliente para o endpoint da cliente VPN, crie uma função do AWS Lambda que utilize os atributos do dispositivo, usuário e conexão como entradas e retorne uma decisão para o serviço da cliente VPN para permitir ou negar uma nova conexão. Especifique a função Lambda no endpoint da cliente VPN. Quando os dispositivos forem conectados ao endpoint da cliente VPN, o serviço da cliente VPN invocará a função Lambda . Somente as conexões autorizadas pela função Lambda podem se conectar ao endpoint da cliente VPN.

> **Note**
>
> Atualmente, o único tipo de manipulador de conexão do cliente compatível é uma função Lambda.

Requisitos e considerações

Veja a seguir requisitos e considerações para o manipulador de conexão do cliente:

- O nome da função Lambda deve começar com o prefixo `AWSClientVPN-`.
- As funções Lambda qualificadas são compatíveis.
- A função Lambda deve estar na mesma AWS região e na mesma AWS conta do endpoint do Client VPN.
- A função Lambda atinge o tempo limite após 30 segundos. Esse valor não pode ser alterado.
- A função Lambda é de forma sincronizada. Ela é invocada depois da autenticação de dispositivo e usuário e antes de as regras de autorização serem avaliadas.
- Se a função Lambda for invocada para uma nova conexão e o serviço da cliente VPN não obtiver uma resposta esperada da função, o serviço da cliente VPN negará a solicitação de conexão. Por exemplo, isso pode ocorrer se a função Lambda for limitada, atingir o tempo limite ou encontrar outros erros inesperados, ou se a resposta da função não estiver em um formato válido.
- Recomendamos configurar a simultaneidade provisionada da função Lambda para permitir que ela seja dimensionada sem flutuações na latência.

- Se você atualizar a função Lambda, as conexões existentes com o endpoint da cliente VPN não serão afetadas. É possível encerrar as conexões existentes e orientar seus clientes a estabelecer novas conexões. Para obter mais informações, consulte Encerrar uma conexão de AWS Client VPN cliente.
- Se os clientes usarem o cliente AWS fornecido para se conectar ao endpoint do Client VPN, eles deverão usar a versão 1.2.6 ou posterior para Windows e a versão 1.2.4 ou posterior para macOS. Para obter mais informações, consulte Conecte-se usando o cliente fornecido pela AWS.

Interface do Lambda

A função Lambda usa atributos de dispositivo, usuário e conexão como entradas do serviço da cliente VPN. Depois, retoma a decisão de permitir ou negar a conexão para o serviço da cliente VPN.

Esquema de solicitação

A função Lambda usa o blob JSON que contém os campos a seguir como entrada.

```
{
    "connection-id": <connection ID>,
    "endpoint-id": <client VPN endpoint ID>,
    "common-name": <cert-common-name>,
    "username": <user identifier>,
    "platform": <OS platform>,
    "platform-version": <OS version>,
    "public-ip": <public IP address>,
    "client-openvpn-version": <client OpenVPN version>,
    "aws-client-version": <AWS client version>,
    "groups": <group identifier>,
    "schema-version": "v3"
}
```

- `connection-id`: o ID da conexão do cliente ao endpoint da cliente VPN.
- `endpoint-id`: o ID do endpoint da cliente VPN.
- `common-name`: o identificador do dispositivo. No certificado do cliente criado para o dispositivo, o nome comum identifica o dispositivo de forma exclusiva.
- `username`: o identificador do usuário, se aplicável. Para autenticação do Active Directory, este é o nome de usuário. Para autenticação federada baseada em SAML, é `NameID`. Para autenticação mútua, este campo fica vazio.

- `platform`: a plataforma do sistema operacional do cliente.
- `platform-version`: a versão do sistema operacional. O serviço da cliente VPN fornece um valor quando a diretiva `--push-peer-info` está presente na configuração do cliente OpenVPN quando ele se conecta a um endpoint da cliente VPN e está executando a plataforma Windows.
- `public-ip`: o endereço IP público do dispositivo de conexão.
- `client-openvpn-version`: a versão do OpenVPN que o cliente está usando.
- `aws-client-version`— A versão AWS do cliente.
- `groups`: o identificador do grupo, se aplicável. Para autenticação do Active Directory, esta será uma lista de grupos do Active Directory. Para autenticação federada baseada em SAML, esta será uma lista de grupos de provedores de identidade (IdP). Para autenticação mútua, este campo fica vazio.
- `schema-version`: a versão do esquema. O padrão é `v3`.

Esquema de resposta

A função Lambda deve retornar os campos a seguir.

```
{
    "allow": boolean,
    "error-msg-on-denied-connection": "",
    "posture-compliance-statuses": [],
    "schema-version": "v3"
}
```

- `allow`: obrigatório. Um booleano (`true` | `false`) que indica se deseja permitir ou negar a nova conexão.
- `error-msg-on-denied-connection`: obrigatório. Uma série de até 255 caracteres que pode ser usada para fornecer etapas e diretrizes para os clientes se a conexão for negada pela função Lambda. No caso de falhas durante a execução da função Lambda (por exemplo, durante a limitação), a seguinte mensagem padrão será apresentada para os clientes.

  ```
  Error establishing connection. Please contact your administrator.
  ```

- `posture-compliance-statuses`: obrigatório. Se você usa a função Lambda para avaliação da postura, esta é uma lista de status para o dispositivo de conexão. Você define os nomes de status de acordo com as categorias de avaliação da postura dos dispositivos, por exemplo, `compliant`,

`quarantined` `unknown` e assim por diante. Os nomes podem ter até 255 caracteres. É possível especificar até 10 status.

- `schema-version`: obrigatório. A versão do esquema. O padrão é `v3`.

É possível usar a mesma função Lambda para vários endpoints da cliente VPN na mesma região.

Para obter mais informações sobre como criar uma função Lambda, consulte a seção Conceitos básicos do AWS Lambda no Guia do desenvolvedor do AWS Lambda .

Utilize o manipulador de conexão do cliente para avaliação da postura

É possível usar o manipulador de conexão do cliente para integrar o endpoint da cliente VPN à solução de gerenciamento de dispositivos existente para avaliar a conformidade da postura dos dispositivos de conexão. Para que a função Lambda funcione como um manipulador de autorização de dispositivo, use a autenticação mútua para o endpoint da cliente VPN. Crie um certificado de cliente exclusivo e uma chave para cada cliente (dispositivo) que se conectará ao endpoint da cliente VPN. A função Lambda pode usar o nome comum exclusivo para o certificado de cliente (que é passado do serviço da cliente VPN) para identificar o dispositivo e buscar o status de conformidade da postura da solução de gerenciamento de dispositivo. É possível usar a autenticação mútua combinada com a autenticação baseada em usuário.

Como alternativa, você pode realizar uma avaliação de postura básica na própria função Lambda. Por exemplo, é possível avaliar os campos `platform` e `platform-version` que são passados para a função Lambda pelo serviço da cliente VPN.

> **Note**
>
> Embora o manipulador de conexão possa ser usado para impor uma versão mínima do AWS Client VPN aplicativo, o campo `aws-client-version` no manipulador de conexão só é aplicável ao AWS Client VPN aplicativo e está sendo preenchido a partir de variáveis de ambiente no dispositivo do usuário.

Habilitar o manipulador de conexão do cliente

Para habilitar o manipulador de conexão do cliente, crie ou modifique um endpoint da Client VPN e especifique o nome do recurso da Amazon (ARN) da função Lambda. Para obter mais informações, consulte Crie um AWS Client VPN endpoint e Modificar um AWS Client VPN endpoint.

Função vinculada ao serviço

AWS Client VPN cria automaticamente uma função vinculada ao serviço em sua conta chamada. AWSServiceRoleForClientVPNConnections A função tem permissões para invocar a função Lambda quando uma conexão é estabelecida com o endpoint da cliente VPN. Para obter mais informações, consulte Usando funções vinculadas a serviços para AWS Client VPN.

Monitore falhas de autorização de conexão

É possível ver o status de autorização de conexões com o endpoint da cliente VPN. Para obter mais informações, consulte Exibir conexões de AWS Client VPN clientes.

Quando o manipulador de conexão do cliente é usado para avaliação da postura, também é possível visualizar os status de conformidade da postura de dispositivos que se conectam ao endpoint da cliente VPN nos logs de conexão. Para obter mais informações, consulte Registro de conexão para um AWS Client VPN endpoint.

Caso um dispositivo falhe na autorização da conexão, o campo `connection-attempt-failure-reason` nos logs de conexão apresentará um dos seguintes motivos de falha:

- `client-connect-failed`: a função Lambda impediu que a conexão fosse estabelecida.
- `client-connect-handler-timed-out`: a função Lambda atingiu o tempo limite.
- `client-connect-handler-other-execution-error`: a função Lambda encontrou um erro inesperado.
- `client-connect-handler-throttled`: a função Lambda foi limitada.
- `client-connect-handler-invalid-response`: a função Lambda retornou uma resposta inválida.
- `client-connect-handler-service-error`: houve um erro no serviço durante a tentativa de conexão.

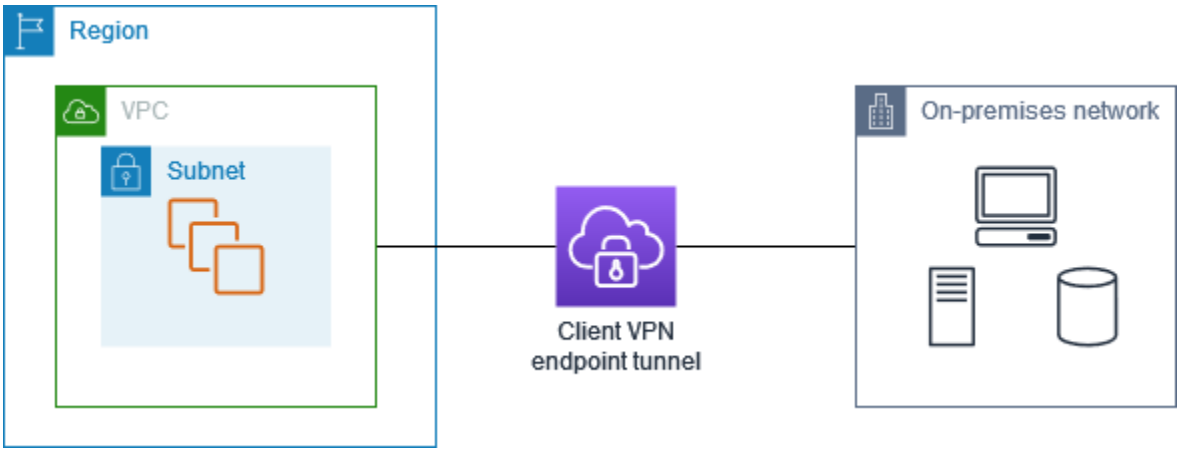
Túnel dividido em endpoints AWS Client VPN

Por padrão, quando você tem um endpoint da Client VPN, todo o tráfego dos clientes é roteado pelo túnel da Client VPN. Quando você habilita o túnel dividido no endpoint da Client VPN, as rotas são enviadas por push na tabela de rotas do endpoint da Client VPN para o dispositivo que está conectado ao endpoint da Client VPN. Isso garante que somente o tráfego com um destino para a

rede correspondente a uma rota da tabela de rotas do endpoint da Client VPN seja roteado pelo do túnel da Client VPN.

É possívelrá usar um endpoint de túnel dividido da Client VPN quando não quiser que todo o tráfego de usuário seja roteado pelo endpoint da Client VPN.

No exemplo a seguir, o túnel dividido está habilitado no endpoint da Client VPN. Somente o tráfego destinado à VPC (`172.31.0.0/16`) é roteado pelo túnel da Client VPN. O tráfego destinado a recursos locais não é roteado pelo túnel da Client VPN.



Benefícios do túnel dividido

O túnel dividido em endpoints da Client VPN oferece os seguintes benefícios:

- Você pode otimizar o roteamento do tráfego dos clientes fazendo com que somente o tráfego AWS destinado atravesse o túnel VPN.
- Você pode reduzir o volume de tráfego de saída e AWS, portanto, reduzir o custo de transferência de dados.

Considerações sobre roteamento

- Ao habilitar o modo de túnel dividido, todas rotas na tabela de rotas do endpoint da Client VPN são adicionadas à tabela de rotas do cliente quando a conexão com a VPN é estabelecida. Essa operação é diferente do comportamento padrão, que substitui a tabela de rotas do cliente pela entrada `0.0.0.0/0` para rotear todo o tráfego pela VPN.

> **Note**
>
> Adicionar uma rota 0.0.0.0/0 à tabela de rotas do endpoint do Client VPN ao usar o modo de túnel dividido pode causar interrupções na conectividade e não é recomendado

- Quando o modo de túnel dividido estiver habilitado, qualquer modificação na tabela de rotas do endpoint da Client VPN resultará na redefinição de todas as conexões do cliente.

Habilitar o túnel dividido

É possível habilitar o túnel dividido em um endpoint novo ou existente da Client VPN. Para obter mais informações, consulte os tópicos a seguir.

- Crie um AWS Client VPN endpoint
- Modificar um AWS Client VPN endpoint

Registro de conexão para um AWS Client VPN endpoint

O registro de conexão é um recurso AWS Client VPN que permite capturar registros de conexão para seu endpoint Client VPN.

Um log de conexão contém entradas de log de conexão que capturam informações sobre eventos de conexão, como quando um cliente (usuário final) se conecta, tenta se conectar ou se desconecta do endpoint da Client VPN. É possível usar essas informações para executar perícia, analisar como seu endpoint da Client VPN está sendo usado ou depurar problemas de conexão.

O registro de conexão está disponível em todas as regiões em AWS Client VPN que está disponível. Os registros de conexão são publicados em um grupo de CloudWatch registros de registros em sua conta.

> **Note**
>
> As tentativas fracassadas de autenticação mútua não são registradas.

Entradas de log de conexão

Uma entrada de log de conexão é um blob em formato JSON de pares de chave/valor. Este é um exemplo de entrada de log de conexão.

```
{
    "connection-log-type": "connection-attempt",
    "connection-attempt-status": "successful",
    "connection-reset-status": "NA",
    "connection-attempt-failure-reason": "NA",
    "connection-id": "cvpn-connection-abc123abc123abc12",
    "client-vpn-endpoint-id": "cvpn-endpoint-aaa111bbb222ccc33",
    "transport-protocol": "udp",
    "connection-start-time": "2020-03-26 20:37:15",
    "connection-last-update-time": "2020-03-26 20:37:15",
    "client-ip": "10.0.1.2",
    "common-name": "client1",
    "device-type": "mac",
    "device-ip": "98.247.202.82",
    "port": "50096",
    "ingress-bytes": "0",
    "egress-bytes": "0",
    "ingress-packets": "0",
    "egress-packets": "0",
    "connection-end-time": "NA",
    "username": "joe"
    }
```

Uma entrada de log de conexão contém as seguintes chaves:

- `connection-log-type`: o tipo de entrada de log de conexão (`connection-attempt` ou `connection-reset`).
- `connection-attempt-status`: o status da solicitação de conexão (`successful`, `failed`, `waiting-for-assertion` ou NA).
- `connection-reset-status`: o status de um evento de redefinição de conexão (NA ou `assertion-received`).
- `connection-attempt-failure-reason`: o motivo da falha de conexão, se aplicável.
- `connection-id`: o ID da conexão.
- `client-vpn-endpoint-id`: o ID do terminal do VPN do Cliente com o qual a conexão foi feita.

- `transport-protocol`: o protocolo de transporte que foi usado para a conexão.
- `connection-start-time`: a hora de início da conexão.
- `connection-last-update-time`: o horário da última atualização da conexão. Esse valor é atualizado periodicamente nos logs.
- `client-ip`— O endereço IP do cliente, que é alocado do intervalo IPv4 CIDR do cliente para o endpoint Client VPN.
- `common-name`: o nome comum do certificado usado para autenticação baseada em certificado.
- `device-type`: o tipo de dispositivo usado para a conexão pelo usuário final.
- `device-ip`: o endereço IP público do dispositivo.
- `port`: o número da porta para a conexão.
- `ingress-bytes`: o número de bytes de entrada para a conexão. Esse valor é atualizado periodicamente nos logs.
- `egress-bytes`: o número de bytes de saída para a conexão. Esse valor é atualizado periodicamente nos logs.
- `ingress-packets`: o número de pacotes de entrada para a conexão. Esse valor é atualizado periodicamente nos logs.
- `egress-packets`: o número de pacotes de saída para a conexão. Esse valor é atualizado periodicamente nos logs.
- `connection-end-time`: a hora de término da conexão. O valor será `NA` se a conexão ainda estiver em andamento ou se a tentativa de conexão falhar.
- `posture-compliance-statuses`: os status da conformidade da postura retornados pelo cliente conectam o manipulador, se aplicável.
- `username`: o nome de usuário é registrado quando a autenticação baseada no usuário (AD ou SAML) é usada para o endpoint.
- `connection-duration-seconds`: a duração de uma conexão em segundos. Igual à diferença entre "connection-start-time" e "connection-end-time”.

Para obter mais informações sobre como habilitar o registro em log de conexão, consulte AWS Client VPN registros de conexão.

Considerações sobre dimensionamento da Client VPN

Ao criar um endpoint da Client VPN, considere o número máximo de conexões VPN simultâneas que você planeja suportar. Você deve levar em conta o número de clientes que você suporta atualmente e se seu endpoint da Client VPN pode ser dimensionado para atender à demanda adicional, se necessário.

Os fatores a seguir afetam o número máximo de conexões VPN simultâneas que podem ser suportadas em um endpoint da Client VPN:

Tamanho do intervalo CIDR do cliente

Ao criar um endpoint Client VPN, você deve especificar um intervalo CIDR do cliente, que é um bloco IPv4 CIDR entre uma máscara de rede /12 e /22. Cada conexão da VPN com o endpoint da Client VPN recebe um endereço IP exclusivo do intervalo CIDR do cliente. Uma parte dos endereços no intervalo de CIDR do cliente também é usada para suportar o modelo de disponibilidade do endpoint da Client VPN e não pode ser atribuída aos clientes. Não é possível alterar o intervalo CIDR do cliente depois de criar o endpoint da Client VPN.

Em geral, recomendamos que você especifique um intervalo CIDR do cliente que contenha o dobro do número de endereços IP (e, portanto, conexões simultâneas) que você planeja suportar no endpoint da Client VPN.

Número de sub-redes associadas

Quando associa uma sub-rede a um endpoint da Client VPN, você permite que os usuários estabeleçam sessões de VPN com o endpoint da Client VPN. É possível associar várias sub-redes a um endpoint da Client VPN para alta disponibilidade e para habilitar a capacidade de conexão adicional.

Veja a seguir o número de conexões VPN simultâneas suportadas com base no número de associações de sub-rede para o endpoint da Client VPN.

Associações de sub-rede	Número suportado de conexões
1	7.000
2	36.500
3	66.500

Associações de sub-rede	Número suportado de conexões
4	96.500
5	126.000

Você não pode associar várias sub-redes da mesma Zona de disponibilidade a um endpoint da Client VPN. Portanto, o número de associações de sub-rede também depende do número de zonas de disponibilidade disponíveis em uma AWS região.

Por exemplo, se você espera suportar 8.000 conexões VPN ao endpoint do Cliente VPN, especifique um tamanho mínimo de intervalo CIDR do cliente de `/18` (16.384 endereços IP) e associe pelo menos 2 sub-redes ao endpoint da Client VPN.

Se você não tiver certeza de qual é o número de conexões VPN esperadas para o endpoint da Client VPN, recomendamos que você especifique um bloco CIDR com um tamanho de `/16` ou maior.

Para obter mais informações sobre as regras e limitações para trabalhar com intervalos CIDR do cliente e redes de destino, consulte Regras e práticas recomendadas para utilizar o AWS Client VPN.

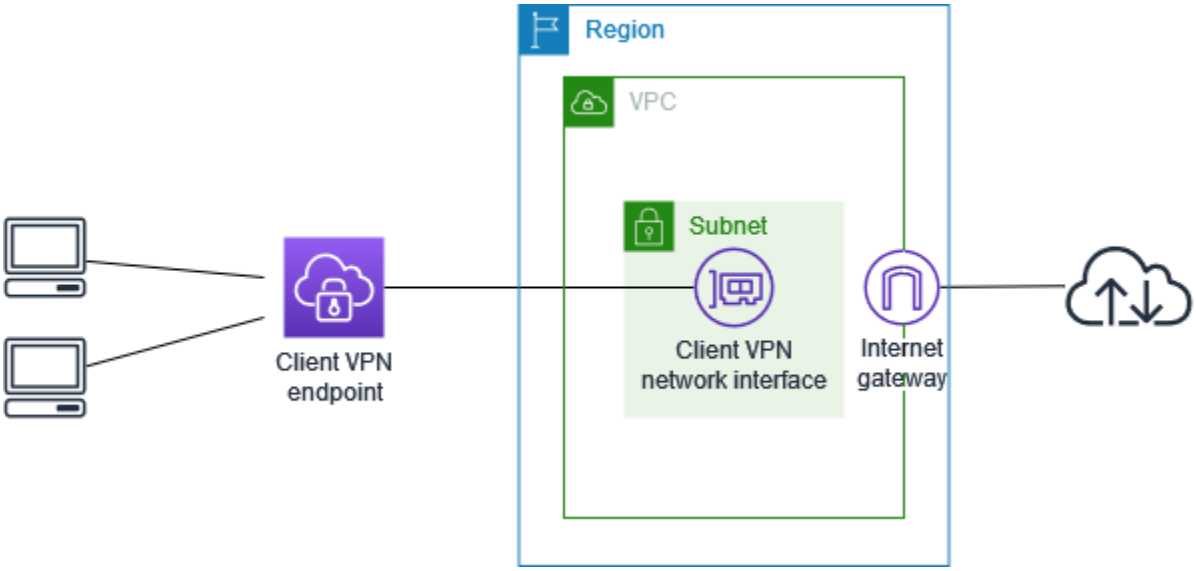
Para obter mais informações sobre cotas para o endpoint da Client VPN, consulte AWS Client VPN cotas.

Comece com AWS Client VPN

Neste tutorial, você criará um AWS Client VPN endpoint que faz o seguinte:

- Fornece a todos os clientes acesso a uma única VPC.
- Fornece a todos os clientes acesso à Internet.
- Usa autenticação mútua.

O diagrama a seguir representa a configuração da VPC e do endpoint da cliente VPN depois da conclusão deste tutorial.



Etapas

- Pré-requisitos
- Etapa 1: gerar chaves e certificados de servidor e cliente
- Etapa 2: Criar um endpoint da Client VPN
- Etapa 3: associar uma rede de destino
- Etapa 4: adicionar uma regra de autorização para a VPC
- Etapa 5: conceder acesso à Internet
- Etapa 6: verificar os requisitos do grupo de segurança
- Etapa 7: baixar o arquivo de configuração do endpoint da VPN do cliente
- Etapa 8: conectar-se ao endpoint da VPN do cliente

Pré-requisitos

Antes de começar este tutorial de conceitos básicos, verifique se você tem o seguinte:

- As permissões necessárias para trabalhar com endpoints da Client VPN.
- As permissões necessárias para importar certificados no AWS Certificate Manager.
- Uma VPC com pelo menos uma sub-rede e um gateway da Internet. A tabela de rota associada à sua sub-rede deve ter uma rota para o gateway da Internet.

Etapa 1: gerar chaves e certificados de servidor e cliente

Este tutorial usa a autenticação mútua. Com a autenticação mútua, a VPN do cliente usa certificados para realizar a autenticação entre os clientes e o endpoint da VPN do cliente. Você precisará ter um certificado e uma chave de servidor e pelo menos um certificado e uma chave de cliente. No mínimo, o certificado do servidor precisará ser importado para o AWS Certificate Manager (ACM) e especificado quando você criar o endpoint Client VPN. A importação do certificado do cliente para o ACM é opcional.

Se você ainda não tiver certificados para usar para esse fim, eles poderão ser criados usando o utilitário easy-rsa do OpenVPN. Para obter as etapas detalhadas de geração dos certificados e das chaves de servidor e cliente usando o utilitário easy-rsa do OpenVPN e obter instruções sobre como importá-los para o ACM, consulte Autenticação mútua em AWS Client VPN.

> **Note**
>
> O certificado do servidor deve ser provisionado ou importado para o AWS Certificate Manager (ACM) na mesma AWS região em que você criará o endpoint do Client VPN.

Etapa 2: Criar um endpoint da Client VPN

O endpoint do cliente VPN é o recurso que você cria e configura para habilitar e gerenciar sessões do cliente VPN. É o ponto de término de todas as sessões da VPN do cliente.

Como criar um endpoint da Client VPN

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, escolha Client VPN Endpoints (Endpoints da VPN do cliente) e escolha Create Client VPN endpoint (Criar endpoint da VPN do cliente).
3. (Opcional) Forneça uma etiqueta de nome e uma descrição para o endpoint da VPN do cliente.
4. Para o IPv4 CIDR do cliente, especifique um intervalo de endereços IP, na notação CIDR, a partir do qual atribuir endereços IP do cliente.

   > **Note**
   >
   > O intervalo de endereços não pode se sobrepor ao intervalo de endereços da rede de destino, ao intervalo de endereços da VPC nem a nenhuma das rotas que serão associadas ao endpoint da VPN do cliente. O intervalo de endereços do cliente deve ser de, no mínimo, /22 e não maior que o tamanho do bloco CIDR /12. Não é possível alterar o intervalo de endereços do cliente depois de criar o endpoint da VPN do cliente.

5. Em Server certificate ARN (ARN do certificado do servidor), selecione o ARN do certificado do servidor gerado na Etapa 1.
6. Em Opções de autenticação, escolha Usar autenticação mútua e, em ARN do certificado do cliente, escolha o ARN do certificado que você deseja usar como o certificado do cliente.

   Se os certificados do servidor e do cliente forem assinados pela mesma autoridade de certificação (CA), você terá a opção de especificar o ARN do certificado do servidor tanto para os certificados do cliente como para os do servidor. Nesse cenário, qualquer certificado do cliente que corresponda ao certificado do servidor pode ser usado para autenticar.

7. (Opcional) Especifique quais servidores DNS devem ser usados para a resolução de DNS. Para usar servidores DNS personalizados, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) e DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP dos servidores DNS a serem usados. Para usar o servidor DNS da VPC, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) ou DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP e adicione o endereço IP do servidor DNS da VPC.

   > **Note**
   >
   > Verifique se os servidores DNS possam ser acessados pelos clientes.

8. Mantenha o restante das configurações padrão e selecione Create Client VPN endpoint (Criar endpoint da VPN do cliente).

Depois que você cria o endpoint da cliente VPN, seu estado é `pending-associate`. Os clientes somente poderão estabelecer uma conexão VPN depois que você associar pelo menos uma rede de destino.

Para obter mais informações sobre as opções que você pode especificar para um endpoint da Client VPN, consulte Crie um AWS Client VPN endpoint.

Etapa 3: associar uma rede de destino

Para permitir que os clientes estabeleçam uma sessão de VPN, associe uma rede de destino ao endpoint da VPN do cliente. Uma rede de destino é uma sub-rede em uma VPC.

Como associar uma rede de destino a um endpoint da VPN do cliente

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da VPN do cliente que você criou no procedimento anterior e escolha Target network associations (Associações de rede de destino), Associate target network (Associar rede de destino).
4. Para VPC, selecione a VPC na qual a sub-rede está localizada.
5. Em Choose a subnet to associate (Escolher uma sub-rede para associar), escolha a sub-rede a ser associada ao endpoint da VPN do cliente.
6. SelecioneAssociate target network (Associar rede de destino).
7. Se as regras de autorização permitirem, uma associação de sub-rede é suficiente para que os clientes acessem toda a rede de uma VPC. É possível associar outras sub-redes para fornecer alta disponibilidade caso uma zona de disponibilidade tenha algum problema.

Quando você associa a primeira sub-rede ao endpoint da Client VPN, acontece o seguinte:

- O estado do endpoint da cliente VPN muda para `available`. Agora, os clientes podem estabelecer uma conexão VPN, mas não poderão acessar recursos na VPC até que você adicione as regras de autorização.
- A rota local da VPC é adicionada automaticamente à tabela de rotas do endpoint da Client VPN.
- O grupo de segurança padrão da VPC é aplicado automaticamente ao endpoint da VPN do cliente.

Etapa 4: adicionar uma regra de autorização para a VPC

Para que os clientes acessem a VPC, é preciso haver uma rota para a VPC na tabela de rotas do endpoint da VPN do cliente e uma regra de autorização. A rota já foi adicionada automaticamente na etapa anterior. Neste tutorial, queremos conceder acesso à VPC para todos os usuários.

Como adicionar uma regra de autorização para a VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Escolha o endpoint da VPN do cliente ao qual deseja adicionar a regra de autorização. Escolha Authorization rules (Regras de autorização) e Add authorization rule (Adicionar regra de autorização).
4. Em Destination network to enable access (Rede de destino para permitir acesso), insira o CIDR da rede à qual você deseja permitir acesso. Por exemplo, para permitir o acesso a toda a VPC, especifique o bloco IPv4 CIDR da VPC.
5. Para Conceder acesso a, escolha Permitir acesso a todos os usuários.
6. (Opcional) Em Description (Descrição), insira uma breve descrição da regra de autorização.
7. Escolha Adicionar regra de autorização.

Etapa 5: conceder acesso à Internet

Você pode fornecer acesso a redes adicionais conectadas à VPC, como AWS serviços, redes com peering VPCs, redes locais e a Internet. Para cada rede adicional, adicione uma rota à rede na tabela de rotas do endpoint da VPN do cliente e configure uma regra de autorização para conceder acesso aos clientes.

Neste tutorial, queremos conceder acesso à Internet e também à VPC para todos os usuários. Você já configurou o acesso à VPC, portanto, essa etapa é para acesso à Internet.

Como conceder acesso à Internet

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Escolha o endpoint da VPN do cliente que você criou para este tutorial. Escolha Route Table (Tabela de rotas) e Create Route (Criar rota).

4. Em Destino da rota, insira `0.0.0.0/0`. Em Subnet ID for target network association (ID da sub-rede para a associação da rede de destino), especifique o ID da sub-rede pela qual deseja encaminhar o tráfego.
5. Escolha Criar rota.
6. Escolha Authorization rules (Regras de autorização) e Add authorization rule (Adicionar regra de autorização).
7. Em Destination network to enable access (Rede de destino para permitir acesso), insira `0.0.0.0/0` e escolha Allow access to all users (Permitir acesso a todos os usuários).
8. Escolha Adicionar regra de autorização.

Etapa 6: verificar os requisitos do grupo de segurança

Neste tutorial, nenhum grupo de segurança foi especificado durante a criação do endpoint da VPN do cliente na Etapa 2. Isso significa que o grupo de segurança padrão da VPC é aplicado automaticamente ao endpoint da VPN do cliente quando uma rede de destino é associada. Como resultado, o grupo de segurança padrão da VPC agora deve estar associado ao endpoint da VPN do cliente.

Verificar os requisitos de grupo de segurança a seguir

- O grupo de segurança associado à sub-rede pela qual você está roteando tráfego (nesse caso, o grupo de segurança da VPC padrão) deve permitir tráfego de saída para a Internet. Para fazer isso, adicione uma regra de saída que permita todo o tráfego para o destino `0.0.0.0/0`.
- Os grupos de segurança para os recursos na VPC devem ter uma regra que permita o acesso do grupo de segurança aplicado ao endpoint da VPN do cliente (nesse caso, o grupo de segurança da VPC padrão). Isso permite que os clientes acessem os recursos na VPC.

Para obter mais informações, consulte Grupos de segurança.

Etapa 7: baixar o arquivo de configuração do endpoint da VPN do cliente

A próxima etapa é baixar o arquivo de configuração do endpoint da VPN do cliente e prepará-lo. O arquivo de configuração inclui os detalhes do endpoint da VPN do cliente e as informações de certificado necessárias para estabelecer uma conexão VPN. Forneça esse arquivo aos usuários

finais que precisam se conectar ao endpoint da VPN do cliente. O usuário final usa o arquivo para configurar a aplicação da VPN do cliente.

Como baixar o arquivo de configuração do endpoint da Client VPN e prepará-lo

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da VPN que você criou para este tutorial e escolha Download client configuration (Baixar a configuração do cliente).
4. Localize o certificado de cliente e a chave que foram gerados na etapa 1. A chave e o certificado de cliente estão disponíveis nos seguintes locais no repositório clonado OpenVPN easy-rsa:
   - Certificado do cliente — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - Chave do cliente — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. Abra o arquivo de configuração do endpoint da Client VPN usando seu editor de texto preferido. Adicione as etiquetas `<cert></cert>` e `<key></key>` ao arquivo. Coloque o conteúdo do certificado do cliente e o conteúdo da chave privada entre as etiquetas correspondentes, como:

```
<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>
```

6. Salve e feche o arquivo de configuração do endpoint da Client VPN.
7. Distribua o arquivo de configuração do endpoint da VPN do cliente para os usuários finais.

Para obter mais informações sobre o arquivo de configuração do endpoint da cliente VPN, consulte AWS Client VPN exportação do arquivo de configuração do endpoint.

Etapa 8: conectar-se ao endpoint da VPN do cliente

Você pode se conectar ao endpoint do Client VPN usando o cliente AWS fornecido ou outro aplicativo cliente baseado em OpenVPN e o arquivo de configuração que você acabou de criar. Para obter mais informações, consulte o Guia do usuário do AWS Client VPN.

Trabalhe com AWS Client VPN

Os tópicos a seguir explicam as principais tarefas administrativas necessárias para trabalhar com a Client VPN:

- Acesse o portal de autoatendimento: configure o acesso ao portal de autoatendimento da Client VPN para que os próprios clientes possam baixar o arquivo de configuração do endpoint da Client VPN. Para obter informações sobre como acessar o portal de autoatendimento, consulte the section called “Acesso ao portal de autoatendimento”.
- Regras de autorização: adicione regras de autorização para controlar o acesso do cliente às redes especificadas. Para obter informações sobre como adicionar regras de autorização, consulte the section called “Regras de autorização”.
- Listas de revogação de certificados de cliente: use listas de revogação de certificados de cliente para revogar o acesso a um endpoint da Client VPN. Para obter informações sobre listas de revogação de certificados de cliente, consulte the section called “Listas de revogação de certificados de cliente”.
- Conexões do cliente: visualize ou encerre uma conexão do cliente com um endpoint da Client VPN. Para obter informações sobre como visualizar ou encerrar uma conexão de cliente, consulte the section called “Conexões de cliente”.
- Banner de login do cliente: adicione um banner de texto em uma aplicação de desktop da Client VPN. É possível utilizar do banner de texto de modo a atender às suas necessidades regulamentares e de conformidade. Para obter informações sobre banners de login, consulte the section called “Banners de login do cliente ”.
- Aplicação de rotas do cliente — aplique rotas definidas pelo administrador em dispositivos conectados por meio da VPN. Para obter mais informações sobre o Client Route Enforcement, consultethe section called “Trabalhando com o Client Route Enforcement”.
- Endpoints da Client VPN: configure os endpoints da Client VPN para gerenciar e controlar todas as sessões VPN. Para obter informações sobre como configurar endpoints, consulte the section called “Endpoints”.
- Logs de conexão: habilite o log de conexão para endpoints da Client VPN novos ou existentes para começar a capturar logs de conexão. Para obter informações sobre o log de conexão, consulte the section called “Logs de conexão”.
- Exportação do arquivo de configuração do cliente: configure o arquivo de configuração do cliente que os clientes da Client VPN precisam para estabelecer conexões VPN. Depois de configurar o arquivo, baixe-o (exporte-o) para distribui-lo aos clientes. Para obter mais informações sobre como

exportar um arquivo de configuração do cliente, consulte the section called “Exportação de arquivo de configuração do cliente”.

- Rotas: configure regras de autorização para cada rota da Client VPN para especificar quais clientes têm acesso à rede de destino. Para obter informações sobre como configurar regras de autorização, consulte the section called “Regras de autorização”.
- Redes de destino: associe as redes de destino a um endpoint da Client VPN para permitir que os clientes se conectar a ele e estabeleçam uma conexão VPN. Para obter informações sobre redes de destino, consulte the section called “Redes de destino”.
- Duração máxima da sessão VPN: defina opções para a duração máxima da sessão VPN de modo a atender aos requisitos de segurança e conformidade. Para obter informações sobre a duração máxima da sessão VPN, consulte the section called “Duração máxima da sessão VPN ”.

AWS Client VPN acesso ao portal de autoatendimento

Se você ativou o portal de autoatendimento para o endpoint da Client VPN, é possível fornecer um URL do portal de autoatendimento para seus clientes. Os clientes podem acessar o portal no navegador da Web e usar as credenciais baseadas em usuário para fazer login. No portal, os clientes podem baixar o arquivo de configuração do endpoint do Client VPN e podem baixar a versão mais recente do cliente AWS fornecido.

As seguintes regras se aplicam:

- O portal de autoatendimento não está disponível para clientes autenticados usando a autenticação mútua.
- O arquivo de configuração que está disponível no portal de autoatendimento é o mesmo arquivo de configuração que você exporta usando o console da Amazon VPC ou. AWS CLI Caso seja necessário personalizar o arquivo de configuração antes de distribuí-lo aos clientes, essa distribuição deverá ser feita por você.
- É necessário habilitar a opção do portal de autoatendimento para o endpoint da Client VPN ou os clientes não conseguirão acessar o portal. Se esta opção não estiver ativada, você poderá modificar o endpoint da Client VPN para ativá-lo.

Depois de habilitar a opção de portal de autoatendimento, forneça aos seus clientes uma das seguintes opções: URLs

- `https://self-service.clientvpn.amazonaws.com/`

Se os clientes acessarem o portal usando esse URL, será necessário inserir o ID do endpoint da Client VPN antes que eles possam fazer login.

- `https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>`

  `<endpoint-id>`Substitua o URL anterior pelo ID do seu endpoint Client VPN, por exemplo,. `cvpn-endpoint-0123456abcd123456`

Você também pode visualizar a URL do portal de autoatendimento na saída do describe-client-vpn-endpoints AWS CLI comando. Como alternativa, o URL está disponível na guia Details (Detalhes) na página Client VPN Endpoints (Endpoints da VPN do cliente) no console da Amazon VPC.

Para obter mais informações sobre como configurar o portal de autoatendimento para uso com a autenticação federada, consulte Suporte para o portal de autoatendimento.

AWS Client VPN regras de autorização

Regras de autorização atuam como regras de firewall que concedem acesso a redes. Adicionando regras de autorização, você concede acesso à rede especificada a clientes específicos. Você deve ter uma regra de autorização para cada rede à qual deseja conceder acesso. É possível adicionar regras de autorização a um endpoint da Client VPN usando o console e a AWS CLI.

> **Note**
>
> O cliente VPN usa a correspondência de prefixo mais longa ao avaliar as regras de autorização. Consulte o tópico sobre solução de problemas Solução de problemas AWS Client VPN: as regras de autorização para grupos do Active Directory não funcionam conforme o esperado e Prioridade de rota no Guia do usuário do Amazon VPC para obter mais detalhes.

Pontos-chave para entender as regras de autorização

Os seguintes pontos explicam alguns dos comportamentos das regras de autorização:

- Para permitir o acesso a uma rede de destino, é necessário adicionar explicitamente uma regra de autorização. O comportamento padrão é negar acesso.
- Você não pode adicionar uma regra de autorização para restringir acesso a uma rede de destino.

- O CIDR `0.0.0.0/0` é tratado como um caso especial. Ele é processado por último, independentemente da ordem na qual as regras de autorização foram criadas.
- O CIDR `0.0.0.0/0` pode ser considerado como “qualquer destino” ou “qualquer destino não definido por outras regras de autorização”.
- A correspondência de prefixo mais longo é a regra que tem precedência.

Tópicos

- Cenários de exemplo para regras de autorização da Client VPN
- Adicionar uma regra de autorização a um endpoint do AWS Client VPN
- Remover uma regra de autorização de um endpoint do AWS Client VPN
- Exibir regras AWS Client VPN de autorização

Cenários de exemplo para regras de autorização da Client VPN

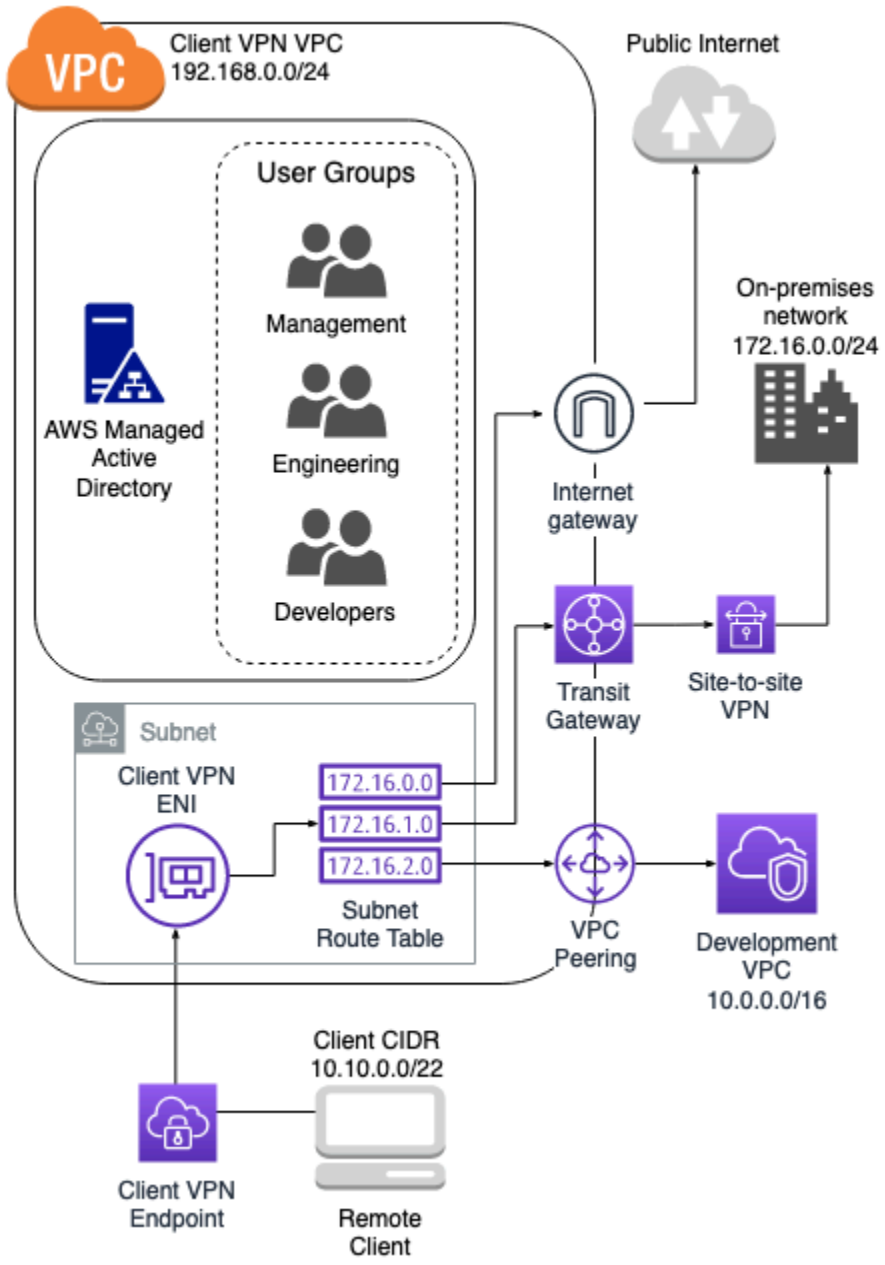
Esta seção descreve como as regras de autorização funcionam para AWS Client VPN. Ela inclui pontos-chave para entender as regras de autorização, um exemplo de arquitetura e uma discussão sobre cenários que correspondem à arquitetura de exemplo.

Cenários

- the section called “Arquitetura de exemplo”
- the section called “Acesso a um único destino”
- the section called “Use qualquer CIDR de destino (0.0.0.0/0)”
- the section called “Correspondência de prefixo de IP mais longo”
- the section called “Sobrepor CIDR (mesmo grupo)”
- the section called “Regra 0.0.0.0/0 adicional”
- the section called “Adicionar regra para 192.168.0.0/24”
- the section called “Acesso para todos os grupos de usuários”

Exemplo de arquitetura para cenários de regras de autorização

O diagrama a seguir mostra a arquitetura de exemplo usada para os cenários encontrados nesta seção.



Acesso a um único destino

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino
Fornecer ao grupo de desenvolvimento acesso à VPC de desenvolvimento	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso à VPC de VPN cliente	S-xxxxx16	Falso	192.168.0.0/24

Comportamento resultante

- O grupo de engenharia somente pode acessar `172.16.0.0/24`.
- O grupo de desenvolvimento somente pode acessar `10.0.0.0/16`.
- O grupo de gerentes somente pode acessar `192.168.0.0/24`.
- Qualquer outro tráfego é descartado pelo endpoint da VPN cliente.

> **Note**
>
> Nesse cenário, nenhum grupo de usuários tem acesso à Internet pública.

Use qualquer CIDR de destino (0.0.0.0/0)

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino
Fornecer ao grupo de desenvolvimento acesso à VPC de desenvolvimento	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso a qualquer destino	S-xxxxx16	Falso	0.0.0.0/0

Comportamento resultante

- O grupo de engenharia somente pode acessar `172.16.0.0/24`.
- O grupo de desenvolvimento só pode acessar `10.0.0.0/16`.
- O grupo de gerentes pode acessar a Internet pública e `192.168.0.0/24`, mas não pode acessar `172.16.0.0/24` nem `10.0.0/16`.

> **Note**
>
> Nesse cenário, como nenhuma regra está se referindo a `192.168.0.0/24`, o acesso a essa rede também é fornecido pela regra `0.0.0.0/0`.
> Uma regra com `0.0.0.0/0` é sempre avaliada por último, independentemente da ordem em que as regras foram criadas. Por esse motivo, lembre-se de que as regras avaliadas antes de `0.0.0.0/0` desempenham um papel na determinação das redes às quais `0.0.0.0/0` concede acesso.

Correspondência de prefixo de IP mais longo

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24
Fornecer ao grupo de desenvolvimento acesso à VPC de desenvolvimento	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso a qualquer destino	S-xxxxx16	Falso	0.0.0.0/0
Fornecer ao grupo de gerentes acesso a um único host na VPC de desenvolvimento	S-xxxxx16	Falso	10.0.2.119/32

Comportamento resultante

- O grupo de engenharia só pode acessar `172.16.0.0/24`.
- O grupo de desenvolvimento pode acessar `10.0.0.0/16`, exceto o único host `10.0.2.119/32`.
- O grupo de gerentes pode acessar a Internet pública, `192.168.0.0/24` e um único host (`10.0.2.119/32`) na VPC de desenvolvimento, mas não tem acesso a `172.16.0.0/24` nem aos hosts restantes na VPC de desenvolvimento.

> **Note**
>
> Aqui, você vê como uma regra com um prefixo de IP mais longo tem precedência sobre uma regra com um prefixo de IP mais curto. Se você quiser que o grupo de desenvolvimento

tenha acesso a `10.0.2.119/32`, é necessário adicionar mais uma regra que conceda à equipe de desenvolvimento acesso a `10.0.2.119/32`.

Sobrepor CIDR (mesmo grupo)

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24
Fornecer ao grupo de desenvolvimento acesso à VPC de desenvolvimento	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso a qualquer destino	S-xxxxx16	Falso	0.0.0.0/0
Fornecer ao grupo de gerentes acesso a um único host na VPC de desenvolvimento	S-xxxxx16	Falso	10.0.2.119/32
Fornecer ao grupo de engenharia acesso a uma sub-rede menor na rede on-premises	S-xxxxx14	Falso	172.16.0.128/25

Comportamento resultante

- O grupo de desenvolvimento pode acessar `10.0.0.0/16`, exceto o único host `10.0.2.119/32`.
- O grupo de gerentes pode acessar a Internet pública, `192.168.0.0/24` e um único host (`10.0.2.119/32`) na rede `10.0.0.0/16`, mas não tem acesso a `172.16.0.0/24` nem aos hosts restantes na rede `10.0.0.0/16`.
- O grupo de engenharia tem acesso a `172.16.0.0/24`, inclusive à sub-rede mais específica `172.16.0.128/25`.

Regra 0.0.0.0/0 adicional

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24
Fornecer ao grupo de desenvolvimento acesso à VPC de desenvolvimento	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso a qualquer destino	S-xxxxx16	Falso	0.0.0.0/0
Fornecer ao grupo de gerentes acesso a um único host na VPC de desenvolvimento	S-xxxxx16	Falso	10.0.2.119/32
Fornecer ao grupo de engenharia acesso a	S-xxxxx14	Falso	172.16.0.128/25

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino
uma sub-rede menor na rede on-premises			
Fornecer ao grupo de engenharia acesso a qualquer destino	S-xxxxx14	Falso	0.0.0.0/0

Comportamento resultante

- O grupo de desenvolvimento pode acessar `10.0.0.0/16`, exceto o único host `10.0.2.119/32`.
- O grupo de gerentes pode acessar a Internet pública, `192.168.0.0/24` e um único host (`10.0.2.119/32`) na rede `10.0.0.0/16`, mas não tem acesso a `172.16.0.0/24` nem aos hosts restantes na rede `10.0.0.0/16`.
- O grupo de engenharia pode acessar a Internet pública, `192.168.0.0/24` e `172.16.0.0/24`, inclusive a sub-rede mais específica `172.16.0.128/25`.

> **Note**
>
> Observe que os grupos de engenharia e de gerentes agora podem acessar `192.168.0.0/24`. Isso ocorre porque os dois grupos têm acesso a `0.0.0.0/0` (qualquer destino) e nenhuma outra regra está fazendo referência a `192.168.0.0/24`.

Adicionar regra para 192.168.0.0/24

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino
Fornecer ao grupo de desenvolvimento acesso à VPC de desenvolvimento	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso a qualquer destino	S-xxxxx16	Falso	0.0.0.0/0
Fornecer ao grupo de gerentes acesso a um único host na VPC de desenvolvimento	S-xxxxx16	Falso	10.0.2.119/32
Fornecer ao grupo de engenharia acesso a uma sub-rede na rede on-premises	S-xxxxx14	Falso	172.16.0.128/25
Fornecer ao grupo de engenharia acesso a qualquer destino	S-xxxxx14	Falso	0.0.0.0/0
Fornecer ao grupo de gerentes acesso à VPC de VPN cliente	S-xxxxx16	Falso	192.168.0.0/24

Comportamento resultante

- O grupo de desenvolvimento pode acessar `10.0.0.0/16`, exceto o único host `10.0.2.119/32`.

- O grupo de gerentes pode acessar a Internet pública, `192.168.0.0/24` e um único host (`10.0.2.119/32`) na rede `10.0.0.0/16`, mas não tem acesso a `172.16.0.0/24` nem aos hosts restantes na rede `10.0.0.0/16`.
- O grupo de engenharia pode acessar a Internet pública, `172.16.0.0/24` e `172.16.0.128/25`.

> **Note**
>
> Observe que a adição da regra para o grupo de gerentes acessar`192.168.0.0/24` faz com que o grupo de desenvolvimento não tenha mais acesso a essa rede de destino.

Acesso para todos os grupos de usuários

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino
Fornecer ao grupo de engenharia acesso à rede on-premises	S-xxxxx14	Falso	172.16.0.0/24
Fornecer ao grupo de desenvolvimento acesso à VPC de desenvolvimento	S-xxxxx15	Falso	10.0.0.0/16
Fornecer ao grupo de gerentes acesso a qualquer destino	S-xxxxx16	Falso	0.0.0.0/0
Fornecer ao grupo de gerentes acesso a um único host na VPC de desenvolvimento	S-xxxxx16	Falso	10.0.2.119/32

Descrição da regra	ID do grupo	Permitir acesso a todos os usuários	CIDR de destino
Fornecer ao grupo de engenharia acesso a uma sub-rede na rede on-premises	S-xxxxx14	Falso	172.16.0.128/25
Fornecer ao grupo de engenharia acesso a todas as redes	S-xxxxx14	Falso	0.0.0.0/0
Fornecer ao grupo de gerentes acesso à VPC de VPN cliente	S-xxxxx16	Falso	192.168.0.0/24
Fornecer acesso a todos os grupos	N/D	Verdadeiro	0.0.0.0/0

Comportamento resultante

- O grupo de desenvolvimento pode acessar `10.0.0.0/16`, exceto o único host `10.0.2.119/32`.
- O grupo de gerentes pode acessar a Internet pública, `192.168.0.0/24` e um único host (`10.0.2.119/32`) na rede `10.0.0.0/16`, mas não tem acesso a `172.16.0.0/24` nem aos hosts restantes na rede `10.0.0.0/16`.
- O grupo de engenharia pode acessar a Internet pública, `172.16.0.0/24` e `172.16.0.128/25`.
- Qualquer outro grupo de usuários, por exemplo, “grupo de administradores”, pode acessar a Internet pública, mas nenhuma outra rede de destino definida nas outras regras.

Adicionar uma regra de autorização a um endpoint do AWS Client VPN

É possível adicionar uma regra de autorização para conceder ou restringir o acesso a um endpoint da Client VPN usando o AWS Management Console. Uma regra de autorização pode ser adicionada a um endpoint da Client VPN usando o console da Amazon VPC ou a linha de comando ou a API.

Para adicionar uma regra de autorização a um endpoint do Client VPN usando AWS Management Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da VPN do cliente ao qual a regra de autorização deve ser adicionada, escolha Authorization rules (Regras de autorização) e Add authorization rule (Adicionar regra de autorização).
4. Em Destination network to enable access (Rede de destino para habilitar o acesso), insira o endereço IP, em notação CIDR, da rede que você deseja que os usuários acessem (por exemplo, o bloco CIDR da VPC).
5. Especifique quais clientes têm permissão para acessar a rede especificada. Em For grant access to (Para conceder acesso a), siga um destes procedimentos:
   - Para conceder acesso a todos os clientes, escolha Allow access to all users (Permitir acesso a todos os usuários).
   - Para restringir o acesso a clientes específicos, escolha Permitir acesso a usuários em um grupo de acesso específico e, em ID do grupo de acesso, insira o ID do grupo ao qual conceder acesso. Por exemplo, o identificador de segurança (SID) de um grupo do Active Directory ou o ID/nome de um grupo definido em um provedor de identidades (IdP) baseado em SAML.
     - (Active Directory) Para obter o SID, você pode usar o ADGroup cmdlet Get- do Microsoft Powershell, por exemplo:

       ```
       Get-ADGroup -Filter 'Name -eq "<Name of the AD Group>"'
       ```

       Como alternativa, abra a ferramenta Usuários e Computadores do Active Directory, visualize as propriedades do grupo, acesse a guia Editor de atributos e obtenha o valor de `objectSID`. Se necessário, primeiro selecione View (Visualizar), Advanced Features (Recursos avançados) para habilitar a guia Editor de atributos.
     - (Autenticação federada baseada em SAML) O ID/nome do grupo deve corresponder às informações de atributo de grupo retornadas na declaração SAML.
6. Em Descrição, insira uma breve descrição da regra de autorização.
7. Escolha Adicionar regra de autorização.

Adicionar uma regra de autorização a um endpoint da Client VPN (AWS CLI)

Use o comando authorize-client-vpn-ingress.

Remover uma regra de autorização de um endpoint do AWS Client VPN

É possível remover regras de autorização de um endpoint específico da Client VPN usando o console e o AWS CLI.

Para remover regras de autorização (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da Client VPN ao qual a regra de autorização foi adicionada e escolha Regras de autorização.
4. Selecione a regra de autorização a ser excluída, escolha Remover regra de autorização e escolha Remover regra de autorização novamente para confirmar a exclusão.

Para remover regras de autorização (AWS CLI)

Use o comando revoke-client-vpn-ingress.

Exibir regras AWS Client VPN de autorização

É possível visualizar regras de autorização de um endpoint específico da Client VPN usando o console e a AWS CLI.

Para visualizar regras de autorização (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da VPN do cliente para o qual deseja visualizar regras de autorização e escolha Authorization rules (Regras de autorização).

Para visualizar regras de autorização (AWS CLI)

Use o comando describe-client-vpn-authorization-rules.

AWS Client VPN listas de revogação de certificados de clientes

As listas de revogação de certificados de cliente da Client VPN são usadas para revogar o acesso a um endpoint da Client VPN para certificados de cliente específicos. Você pode gerar uma lista de revogação ou importar uma lista existente. Você também pode exportar sua lista atual como um arquivo de lista de revogação. A geração de uma lista é realizada usando o software OpenVPN no Linux/macOS ou no Windows. A importação e a exportação podem ser feitas usando o console Amazon VPC ou usando a CLI. AWS

Para obter mais informações sobre como gerar os certificados e as chaves de servidor e cliente, consulte Autenticação mútua em AWS Client VPN

> **Note**
>
> Se uma lista de revogação de certificados de cliente tiver expirado, você não poderá se conectar ao endpoint do Client VPN. Você precisará criar um novo e importá-lo para o endpoint do Client VPN.

É possível adicionar somente um número limitado de entradas a uma lista de revogação de certificados de cliente. Para obter mais informações sobre o número de entradas que você pode adicionar a uma lista de revogação, consulte Cotas da Client VPN.

Tarefas

- Gere uma lista de revogação de certificados de AWS Client VPN clientes
- Importar uma lista de revogação de certificados de AWS Client VPN cliente
- Exportar uma AWS Client VPN lista de revogação de certificados de cliente

Gere uma lista de revogação de certificados de AWS Client VPN clientes

É possível gerar uma lista de revogação de certificados da Client VPN em um sistema operacional Linux/macOS ou Windows. A lista de revogação é usada para revogar o acesso a um endpoint da Client VPN para certificados específicos. Para obter mais informações sobre listas de revogação de certificados de cliente, consulte Listas de revogação de certificados de cliente.

Linux/macOS

No procedimento a seguir, gere uma lista de revogação de certificados de cliente usando o utilitário de linha de comando OpenVPN easy-rsa.

Para gerar uma lista de revogação de certificados de cliente usando o OpenVPN easy-rsa

1. Faça login no servidor que hospeda a instalação de easyrsa usada para gerar o certificado.
2. Navegue até a pasta `easy-rsa/easyrsa3` no seu repositório local.

```
$ cd easy-rsa/easyrsa3
```

3. Revogar o certificado de cliente e gerar a lista de revogação de cliente.

```
$ ./easyrsa revoke client1.domain.tld
$ ./easyrsa gen-crl
```

Digite `yes` quando solicitado.

Windows

O procedimento a seguir usa o software OpenVPN para gerar uma lista de revogação de cliente. Ele pressupõe que você seguiu as etapas para usar o software OpenVPN para gerar os certificados e as chaves de cliente e servidor.

Para gerar uma lista de revogação de certificados de cliente usando o EasyRSA versão 3.x.x

1. Abra um prompt de comando e navegue até o diretório EasyRSA-3.x.x, o que dependerá de onde ele estiver instalado no sistema.

```
C:\> cd c:\Users\windows\EasyRSA-3.x.x
```

2. Execute o arquivo `EasyRSA-Start.bat` para iniciar o shell EasyRSA.

```
C:\> .\EasyRSA-Start.bat
```

3. No shell EasyRSA, revogue o certificado do cliente.

```
# ./easyrsa revoke client_certificate_name
```

4. Digite `yes` quando solicitado.
5. Gere a lista de revogação de clientes.

```
# ./easyrsa gen-crl
```

6. A lista de revogação de cliente será criada neste local:

```
c:\Users\windows\EasyRSA-3.x.x\pki\crl.pem
```

Para gerar uma lista de revogação de certificados de cliente usando versões anteriores do EasyRSA

1. Abra um prompt de comando e navegue até o diretório OpenVPN.

```
C:\> cd \Program Files\OpenVPN\easy-rsa
```

2. Execute o arquivo `vars.bat`.

```
C:\> vars
```

3. Revogar o certificado de cliente e gerar a lista de revogação de cliente.

```
C:\> revoke-full client_certificate_name
C:\> more crl.pem
```

Importar uma lista de revogação de certificados de AWS Client VPN cliente

Você deve ter um arquivo de lista de revogação de certificados de cliente da Client VPN para importar. Para obter mais informações sobre como gerar uma lista de revogação de certificados de cliente, consulte Gere uma lista de revogação de certificados de AWS Client VPN clientes.

É possível importar uma lista de revogação de certificados de cliente usando o console e a AWS CLI.

Para importar uma lista de revogação de certificados de cliente (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.

3. Selecione o endpoint da Client VPN para o qual você deseja importar a lista de revogação de certificados de cliente.
4. Escolha Actions (Ações) e Import Client Certificate CRL (Importar CRL de certificados de cliente).
5. Em Certificate Revocation List (Lista de revogação de certificado), insira o conteúdo do arquivo de lista de revogação de certificados de cliente e escolha Import client certificate CRL (Importar CRL de certificados de cliente).

Para importar uma lista de revogação de certificados de cliente (AWS CLI)

Use o certificate-revocation-list comando import-client-vpn-client-.

```
$ aws ec2 import-client-vpn-client-certificate-revocation-list --certificate-
revocation-list file://path_to_CRL_file --client-vpn-endpoint-id endpoint_id --
region region
```

Exportar uma AWS Client VPN lista de revogação de certificados de cliente

É possível exportar listas de revogação de certificados de cliente da Client VPN usando o console e o AWS CLI.

Para exportar uma lista de revogação de certificados de cliente (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da Client VPN para o qual você deseja exportar a lista de revogação de certificados de cliente.
4. Escolha Actions (Ações), Export Client Certificate CRL (Exportar CRL de certificados de cliente) e Export Client Certificate CRL (Exportar CRL de certificados de cliente).

Para exportar uma revogação de certificado de cliente (AWS CLI)

Use o certificate-revocation-list comando export-client-vpn-client-.

AWS Client VPN conexões de clientes

AWS Client VPN conexões são sessões de VPN ativas que foram estabelecidas pelos clientes em um endpoint específico do Client VPN, bem como conexões que foram encerradas nos últimos 60 minutos para esse endpoint. Uma conexão é estabelecida quando um cliente se conecta com êxito a um endpoint da Client VPN. O encerramento de uma sessão encerra a conexão do cliente ao endpoint da Client VPN.

É possível visualizar e encerrar as conexões da Client VPN. A visualização das informações de conexão retorna informações como o endereço IP atribuído pelo intervalo de blocos CIDR do cliente, o ID do endpoint e o timestamp. O encerramento de uma sessão encerra a conexão do cliente ao endpoint da Client VPN. A visualização e o encerramento das sessões podem ser feitos usando o console da Amazon VPC ou a AWS CLI. Se você não conseguir se conectar ao endpoint, e dependendo do erro, consulte Solução de problemas para ver as etapas a serem seguidas para resolver o problema.

Tarefas

- Exibir conexões de AWS Client VPN clientes
- Encerrar uma conexão de AWS Client VPN cliente

Exibir conexões de AWS Client VPN clientes

É possível visualizar as conexões ativas da Client VPN usando o Amazon VPC Console ou a CLI da AWS .

Para visualizar conexões de clientes Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da Client VPN para o qual você deseja visualizar conexões de clientes.
4. Escolha a guia Connections (Conexões). A guia Connections (Conexões) lista todas as conexões de clientes ativas e encerradas.

Para visualizar conexões de clientes da Client VPN (AWS CLI)

Use o comando describe-client-vpn-connections.

Encerrar uma conexão de AWS Client VPN cliente

Você pode encerrar uma conexão de cliente Client VPN usando o console Amazon VPC ou a AWS CLI.

Para encerrar uma conexão de cliente Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da Client VPN ao qual o cliente está conectado e escolha Conexões..
4. Selecione a conexão a ser encerrada, escolha Encerrar conexão e depois Encerrar conexão novamente para confirmar o encerramento.

Para encerrar uma conexão de cliente da Client VPN (AWS CLI)

Use o comando terminate-client-vpn-connections.

AWS Client VPN banners de login de clientes

AWS Client VPN fornece a opção de exibir um banner de texto nos aplicativos de desktop Client VPN AWS fornecidos quando uma sessão de VPN é estabelecida. É possível definir o conteúdo do banner de texto de modo a atender às suas necessidades regulamentares e de conformidade. É possível usar no máximo 1.400 caracteres codificados em UTF-8.

> **Note**
>
> Quando um banner de login do cliente for habilitado, ele será exibido somente em sessões VPN recém-criadas. As sessões VPN existentes não serão interrompidas, mas o banner será exibido quando uma sessão existente for restabelecida.

Criação de banners

Os banners de login são inicialmente criados e ativados durante a criação do endpoint da Client VPN. Para conhecer as etapas para ativar um banner de login do cliente durante a criação de um endpoint da Client VPN, consulte Crie um AWS Client VPN endpoint.

Tarefas

- Configurar um banner de login do cliente para um AWS Client VPN endpoint existente
- Desativar um banner de login do cliente para um endpoint do AWS Client VPN existente
- Modificar o texto do banner existente em um endpoint do AWS Client VPN
- Exibir um banner de AWS Client VPN login atualmente configurado

Configurar um banner de login do cliente para um AWS Client VPN endpoint existente

Realize as etapas a seguir para configurar um banner de login do cliente para um endpoint do cliente VPN existente.

Habilitar banner de login do cliente em um endpoint do cliente VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint do cliente VPN que deseja modificar, escolha Actions (Ações) e escolha Modify Client VPN Endpoint (Modificar endpoint do cliente VPN).
4. Role a página para baixo até a seção Other parameters (Outros parâmetros).
5. Ative Enable client login banner (Habilitar o banner de login do cliente).
6. Para o texto do banner de login do cliente, insira o texto que será exibido em um banner nos clientes AWS fornecidos quando uma sessão de VPN for estabelecida. Use apenas caracteres codificados UTF-8, com um máximo de 1400 caracteres permitidos.
7. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Habilitar banner de login do cliente em um endpoint do cliente VPN (AWS CLI)

Use o comando modify-client-vpn-endpoint.

Desativar um banner de login do cliente para um endpoint do AWS Client VPN existente

Use as etapas a seguir para desativar um banner de login do cliente para um endpoint da VPN do cliente existente.

Desativar o banner de login do cliente em um endpoint da VPN do cliente (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da VPN do cliente que você deseja modificar, escolha Actions (Ações) e Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).
4. Role a página para baixo até a seção Other parameters (Outros parâmetros).
5. Desabilite a opção Habilitar o banner de login do cliente?.
6. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Desativar o banner de login do cliente em um endpoint da VPN do cliente (AWS CLI)

Use o comando modify-client-vpn-endpoint.

Modificar o texto do banner existente em um endpoint do AWS Client VPN

Use as etapas a seguir para modificar o texto existente em um banner de login do cliente Client VPN.

Modificar o texto do banner existente em um endpoint da Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da VPN do cliente que você deseja modificar, escolha Actions (Ações) e Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).
4. Em Enable client login banner? (Habilitar banner de login do cliente?), verifique se essa opção está ativada.
5. Para o texto do banner de login do cliente, substitua o texto existente pelo novo texto que você deseja exibir em um banner nos clientes AWS fornecidos quando uma sessão de VPN for estabelecida. Use apenas caracteres codificados UTF-8, com um máximo de 1400 caracteres.
6. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Modificar banner de login do cliente em um endpoint do cliente VPN (AWS CLI)

Use o comando modify-client-vpn-endpoint.

Exibir um banner de AWS Client VPN login atualmente configurado

Use as etapas a seguir para visualizar um banner de login do cliente Client VPN atualmente configurado.

Visualizar banner de login atual para um endpoint da Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da Client VPN que deseja visualizar.
4. Verifique se a guia Details (Detalhes) está selecionada.
5. Visualize o texto do banner de login configurado atualmente ao lado de Client login banner text (Texto do banner de login do cliente).

Visualizar banner de login configurado atualmente para um endpoint do cliente VPN (AWS CLI)

Use o comando describe-client-vpn-endpoints.

AWS Client VPN Aplicação da rota do cliente

O Client Route Enforcement ajuda a aplicar rotas definidas pelo administrador em dispositivos conectados por meio da VPN. Esse recurso ajuda a melhorar sua postura de segurança, garantindo que o tráfego de rede proveniente de um cliente conectado não seja enviado inadvertidamente para fora do túnel VPN.

O Client Route Enforcement monitora a tabela de roteamento principal do dispositivo conectado e garante que o tráfego de saída da rede vá para um túnel VPN, de acordo com as rotas de rede configuradas no endpoint VPN do cliente. Isso inclui modificar as tabelas de roteamento em um dispositivo se forem detectadas rotas conflitantes com o túnel VPN.

Requisitos

O Client Route Enforcement só funciona com as seguintes versões AWS fornecidas do Client VPN:

- Windows versão 5.2.0 ou superior
- macOS versão 5.2.0 ou superior

- Ubuntu versão 5.2.0 ou superior

Conflitos de roteamento

Enquanto um cliente está conectado à VPN, é feita uma comparação entre a tabela de rotas local do cliente e as rotas de rede do endpoint. Um conflito de roteamento ocorrerá se houver sobreposição de rede entre duas entradas da tabela de rotas. Um exemplo de redes sobrepostas é:

- `172.31.0.0/16`
- `172.31.1.0/24`

Neste exemplo, esses blocos CIDR constituem um conflito de roteamento. Por exemplo, `172.31.0.0/16` pode ser o CIDR do túnel VPN. Como `172.31.1.0/24` é mais específico porque tem um prefixo mais longo, normalmente tem precedência e potencialmente redireciona o tráfego de VPN dentro do intervalo de `172.31.1.0/24` IP para outro destino. Isso pode levar a um comportamento de roteamento não intencional. No entanto, quando o Client Route Enforcement estiver habilitado, o último CIDR será removido. Ao usar esse recurso, possíveis conflitos de roteamento devem ser levados em consideração.

As conexões VPN de túnel completo direcionam todo o tráfego da rede por meio da conexão VPN. Como resultado, os dispositivos conectados à VPN não poderão acessar os recursos da rede local (LAN) se o recurso Client Route Enforcement estiver ativado. Se for necessário acesso à LAN local, considere usar o modo de túnel dividido em vez do modo de túnel completo. Para obter mais informações sobre túnel dividido, consulte. Client VPN de túnel dividido

Considerações

As informações a seguir devem ser levadas em consideração antes de ativar o Client Route Enforcement.

- No momento da conexão, se um conflito de roteamento for detectado, o recurso atualizará a tabela de rotas do cliente para direcionar o tráfego para o túnel VPN. As rotas que existiam antes do estabelecimento da conexão e foram excluídas por esse recurso serão restauradas.
- O recurso é aplicado somente na tabela de roteamento principal e não se aplica a outros mecanismos de roteamento. Por exemplo, a fiscalização não se aplica ao seguinte:
  - roteamento baseado em políticas
  - roteamento com escopo de interface

- O Client Route Enforcement protege o túnel VPN enquanto ele está aberto. Não há proteção depois que o túnel é desconectado ou enquanto o cliente está se reconectando.

Impacto das diretivas do OpenVPN na aplicação do Cloud Route

Algumas diretivas personalizadas no arquivo de configuração do OpenVPN têm interações específicas com o Client Route Enforcement:

- A diretiva `route`
  - Ao adicionar rotas a um gateway VPN. Por exemplo, adicionar a rota `192.168.100.0 255.255.255.0` a um gateway VPN.

    As rotas adicionadas a um gateway de VPN são monitoradas pelo Client Route Enforcement da mesma forma que qualquer outra rota de VPN. Quaisquer rotas conflitantes dentro delas serão detectadas e removidas.
  - Ao adicionar rotas a um gateway não VPN. Por exemplo, adicionar a rota`192.168.200.0 255.255.255.0 net_gateway`.

    As rotas adicionadas a um gateway não VPN são excluídas do Client Route Enforcement, pois elas contornam o túnel VPN. Rotas conflitantes são permitidas dentro delas. No exemplo acima, a rota será excluída do monitoramento pelo Client Route Enforcement.
- A `route-ipv6` diretiva.

  Essa diretiva não é processada, pois o Client Route Enforcement suporta apenas IPv4 endereços.

Rotas ignoradas

As rotas para as seguintes redes serão ignoradas pelo Client Route Enforcement:

- `127.0.0.0/8`— Reservado para o anfitrião local
- `169.254.0.0/16`— Reservado para endereços locais de link
- `224.0.0.0/4`— Reservado para multicast
- `255.255.255.255/32`— Reservado para transmissão

Tópicos

- Ativar o Client Route Enforcement para um AWS Client VPN endpoint

- Desative o Client Route Enforcement a partir de um endpoint AWS Client VPN

Ativar o Client Route Enforcement para um AWS Client VPN endpoint

Você pode ativar o Client Route Enforcement em endpoints Client VPN existentes usando o console ou o. AWS CLI

Para ativar o Client Route Enforcement usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN endpoints (Endpoints da VPN do cliente).
3. Escolha o endpoint do Client VPN que você deseja modificar, escolha Actions e, em seguida, escolha Modify Client VPN endpoint.
4. Role a página para baixo até a seção Other parameters (Outros parâmetros).
5. Ative o Client Route Enforcement.
6. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Para ativar o Client Route Enforcement usando o AWS CLI)

- Use o comando modify-client-vpn-endpoint.

Desative o Client Route Enforcement a partir de um endpoint AWS Client VPN

Você pode desativar o Client Route Enforcement em endpoints do Client VPN usando o console ou o. AWS CLI

Para desativar o Client Route Enforcement usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN endpoints (Endpoints da VPN do cliente).
3. Escolha o endpoint do Client VPN que você deseja modificar, escolha Actions e, em seguida, escolha Modify Client VPN endpoint.
4. Role a página para baixo até a seção Other parameters (Outros parâmetros).
5. Desative a fiscalização da rota do cliente.

6. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Para desativar o Client Route Enforcement usando o AWS CLI

- Use o comando modify-client-vpn-endpoint.

AWS Client VPN endpoints

Todas as AWS Client VPN sessões estabelecem comunicação com um endpoint Client VPN. É possível gerenciar o endpoint da Client VPN para criar, modificar, visualizar e excluir sessões de VPN do cliente com esse endpoint. Os endpoints podem ser criados e modificados usando o console Amazon VPC ou usando a CLI da AWS .

Requisitos para criar endpoints da Client VPN

> **Important**
>
> Um endpoint Client VPN deve ser criado na mesma AWS conta na qual a rede de destino pretendida é provisionada. Você também precisará gerar um certificado do servidor e, se necessário, um certificado do cliente. Para obter mais informações, consulte Autenticação do cliente em AWS Client VPN.

Antes de começar, faça o seguinte:

- Revise as regras e as limitações em Regras e práticas recomendadas para utilizar o AWS Client VPN.
- Gere o certificado do servidor e, se necessário, o certificado do cliente. Para obter mais informações, consulte Autenticação do cliente em AWS Client VPN.

Modificação do endpoint

Após a criação de um Client VPN, é possível modificar qualquer uma das seguintes configurações:

- A descrição
- O certificado de servidor
- As opções de registro em log da conexão do cliente

- A opção do manipulador de conexão do cliente
- Os servidores DNS
- A opção de túnel dividido
- Rotas (ao usar a opção de túnel dividido)
- Lista de revogação de certificados (CRL)
- Regras de autorização
- A VPC e as associações do grupo de segurança
- O número da porta VPN
- A opção do portal de autoatendimento
- Duração máxima da sessão VPN
- Ativar ou desativar a reconexão automática no tempo limite da sessão
- Habilitar ou desabilitar o texto do banner de login do cliente
- Texto do banner de login do cliente

> **Note**
>
> As modificações nos endpoints da Client VPN, incluindo alterações na lista de revogação de certificados (CRL), entrarão em vigor até quatro horas depois que a solicitação for aceita pelo serviça Client VPN.
>
> Você não pode modificar o intervalo IPv4 CIDR do cliente, as opções de autenticação, o certificado do cliente ou o protocolo de transporte após a criação do endpoint do Client VPN.

Quando você modifica qualquer um dos seguintes parâmetros em um endpoint da Client VPN, a conexão é redefinida:

- O certificado de servidor
- Os servidores DNS
- A opção de túnel dividido (ligar ou desligar a compatibilidade)
- Rotas (quando você usa a opção de túnel dividido)
- Lista de revogação de certificados (CRL)
- Regras de autorização

- O número da porta VPN

Tarefas

- Crie um AWS Client VPN endpoint
- Exibir AWS Client VPN endpoints
- Modificar um AWS Client VPN endpoint
- Excluir um AWS Client VPN endpoint

Crie um AWS Client VPN endpoint

Crie um endpoint Client VPN para permitir que seus clientes estabeleçam uma sessão de VPN usando o console Amazon VPC ou o. AWS CLI

Antes de criar um endpoint, familiarize-se com os requisitos. Para obter mais informações, consulte the section called “Requisitos para criar endpoints da Client VPN”.

Para criar um endpoint Client VPN usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN. e escolha Criar endpoint da cliente VPN.
3. (Opcional) Forneça uma etiqueta de nome e uma descrição para o endpoint da VPN do cliente.
4. Para o IPv4 CIDR do cliente, especifique um intervalo de endereços IP, na notação CIDR, a partir do qual atribuir endereços IP do cliente. Por exemplo, .`10.0.0.0/22`

   > **Note**
   >
   > O intervalo de endereços não pode se sobrepor ao intervalo de endereços da rede de destino, ao intervalo de endereços da VPC nem a nenhuma das rotas que serão associadas ao endpoint da VPN do cliente. O intervalo de endereços do cliente deve ser de, no mínimo, /22 e não maior que o tamanho do bloco CIDR /12. Não é possível alterar o intervalo de endereços do cliente depois de criar o endpoint da VPN do cliente.

5. Para ARN do certificado de servidor, especifique o ARN do certificado TLS a ser usado pelo servidor. Os clientes usam o certificado de servidor para autenticar o endpoint da Client VPN. ao qual estão se conectando.

> **Note**
>
> O certificado do servidor deve estar presente AWS Certificate Manager (ACM) na região em que você está criando o endpoint do Client VPN. O certificado pode ser provisionado com o ACM ou importado para o ACM.
> Para obter as etapas para provisionar ou importar um certificado para o ACM, consulte AWS Certificate Manager Certificados no Guia do AWS Certificate Manager Usuário.

6. Especifique o método de autenticação a ser usado para autenticar os clientes quando eles estabelecer uma conexão VPN. Você deve selecionar um método de autenticação.

   - Para utilizar a autenticação baseada no usuário, selecione Utilizar autenticação baseada no usuário e, depois, escolha uma das seguintes opções:
     - Autenticação do Active Directory: escolha esta opção para autenticação do Active Directory. Em ID do diretório, especifique o ID do Active Directory a ser usado.
     - Autenticação federada: escolha esta opção para autenticação federada baseada em SAML.

       Em ARN do provedor SAML, especifique o ARN do provedor de identidade SAML do IAM.

       (Opcional) Em ARN do provedor SAML de autoatendimento, especifique o ARN do provedor de identidade SAML do IAM que você criou para oferecer compatibilidade com o portal de autoatendimento, se aplicável.
   - Para usar a autenticação de certificado mútuo, selecione Usar autenticação mútua e, em seguida, para ARN do certificado do cliente, especifique o ARN do certificado do cliente que está provisionado no (ACM). AWS Certificate Manager

     > **Note**
     >
     > Se os certificados de servidor e cliente tiverem sido emitidos pela mesma autoridade de certificação (CA), você poderá usar o ARN de certificado de servidor para ambos, servidor e cliente. Se o certificado do cliente tiver sido emitido por uma autoridade de certificação diferente, o ARN do certificado do cliente deverá ser especificado.

7. (Opcional) Para registro de conexão, especifique se deseja registrar dados sobre conexões de clientes usando o Amazon CloudWatch Logs. Ative Enable log details on client connections (Habilitar detalhes de log nas conexões de cliente). Em Nome do grupo de CloudWatch registros de registros, insira o nome do grupo de registros a ser usado. Em Nome do fluxo de CloudWatch

registros, insira o nome do fluxo de registros a ser usado ou deixe essa opção em branco para que possamos criar um fluxo de registros para você.

8. (Opcional) Em Client Connect Handler (Manipulador de conexão do cliente), ative Enable client connect handler (Habilitar o manipulador de conexão do cliente) para executar o código personalizado que permite ou nega uma nova conexão com o endpoint da VPN do cliente. Em Client Connect Handler ARN (ARN do manipulador de conexão do cliente), especifique o nome de recurso da Amazon (ARN) da função do Lambda que contém a lógica que permite ou nega conexões.
9. (Opcional) Especifique quais servidores DNS devem ser usados para a resolução de DNS. Para usar servidores DNS personalizados, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) e DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP dos servidores DNS a serem usados. Para usar o servidor DNS da VPC, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) ou DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP e adicione o endereço IP do servidor DNS da VPC.

   > **Note**
   >
   > Verifique se os servidores DNS possam ser acessados pelos clientes.

10. (Opcional) Por padrão, o servidor da VPN do cliente usa o protocolo de transporte `UDP`. Para usar o protocolo de transporte `TCP`, em Transport Protocol (Protocolo de transporte), selecione TCP.

    > **Note**
    >
    > Em geral, o UDP oferece melhor performance que o TCP. Não é possível alterar o protocolo de transporte depois de criar o endpoint da Client VPN.

11. (Opcional) Para que o endpoint seja um endpoint de VPN do cliente de túnel dividido, ative Enable split-tunnel (Habilitar túnel dividido). Por padrão, o túnel dividido em um endpoint da Client VPN está desabilitado.
12. (Opcional) Em VPC ID (ID da VPC), selecione a VPC a ser associada ao endpoint da Client VPN. Em Security Group IDs, escolha um ou mais dos grupos de segurança da VPC para aplicar ao endpoint do Client VPN.
13. (Opcional) Em VPN port (Porta VPN), selecione o número da porta VPN. O padrão é 443.

14. (Opcional) Para gerar um URL do portal de autoatendimento para clientes, ative Enable self-service portal (Habilitar portal de autoatendimento).
15. (Opcional) Em Session timeout hours (Horas do tempo limite da sessão), escolha o tempo máximo desejado de duração da sessão VPN em horas, conforme as opções disponíveis, ou deixe definido como padrão de 24 horas.
16. (Opcional) Em Desconectar no tempo limite da sessão, escolha se você deseja encerrar a sessão quando o tempo máximo da sessão for atingido. A escolha dessa opção exige que os usuários se reconectem manualmente ao endpoint quando a sessão expirar; caso contrário, o Client VPN tentará se reconectar automaticamente.
17. (Opcional) Especifique se deseja habilitar o texto do banner de login do cliente. Ative Enable client login banner (Habilitar o banner de login do cliente). Em Client login banner text (Texto do banner de login do cliente), insira o texto que será exibido em um banner nos clientes fornecidos pela AWS quando uma sessão VPN for estabelecida. Somente caracteres com codificação UTF-8. Máximo de 1400 caracteres.
18. Selecione Create Client VPN endpoint (Criar endpoint da VPN do cliente).

Depois de criar o endpoint da Client VPN, faça o seguinte para concluir a configuração e permitir que os clientes se conectem:

- O estado inicial do endpoint da Client VPN é `pending-associate`. Os clientes poderão se conectar ao endpoint da Client VPN somente depois que você associar a primeira rede de destino.
- Crie uma regra de autorização para especificar quais clientes têm acesso à rede.
- Baixe e prepare o arquivo de configuração do endpoint da Client VPN para distribuir aos seus clientes.
- Instrua seus clientes a usar o cliente AWS fornecido ou outro aplicativo cliente baseado em OpenVPN para se conectar ao endpoint do Client VPN. Para obter mais informações, consulte o Guia do usuário do AWS Client VPN.

Para criar um endpoint Client VPN usando o AWS CLI

Use o comando create-client-vpn-endpoint.

Exibir AWS Client VPN endpoints

É possível visualizar informações sobre endpoints da Client VPN ao usar o Amazon VPC Console ou o AWS CLI.

Como visualizar endpoints da VPN do cliente (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da Client VPN a ser visualizado.
4. Use as guias Details (Detalhes), Target network associations (Associações de rede de destino), Security groups (Grupos de segurança), Authorization rules (Regras de autorização), Route table (Tabela de rotas), Connections (Conexões) e Tags (Etiquetas) para visualizar informações sobre os endpoints da VPN do cliente existentes.

   Você também pode usar filtros para ajudar a refinar a pesquisa.

Como visualizar endpoints da VPN do cliente (AWS CLI)

Use o comando describe-client-vpn-endpoints.

Modificar um AWS Client VPN endpoint

É possível modificar um endpoint da Client VPN usando o Amazon VPC Console ou o AWS CLI. Para obter mais informações sobre os campos da Client VPN que podem ser modificados, consulte the section called “Modificação do endpoint”.

> **Note**
>
> As modificações nos endpoints da Client VPN, incluindo alterações na lista de revogação de certificados (CRL), entrarão em vigor até quatro horas depois que a solicitação for aceita pelo serviça Client VPN.
> Você não pode modificar o intervalo IPv4 CIDR do cliente, as opções de autenticação, o certificado do cliente ou o protocolo de transporte após a criação do endpoint do Client VPN.

Para modificar um endpoint da Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da VPN do cliente a ser modificado, escolha Actions (Ações) e Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).
4. Em Description (Descrição), digite uma breve descrição do endpoint da Client VPN.

5. Para ARN do certificado de servidor, especifique o ARN do certificado TLS a ser usado pelo servidor. Os clientes usam o certificado de servidor para autenticar o endpoint da Client VPN. ao qual estão se conectando.

> **Note**
>
> O certificado do servidor deve estar presente AWS Certificate Manager (ACM) na região em que você está criando o endpoint do Client VPN. O certificado pode ser provisionado com o ACM ou importado para o ACM.

6. Especifique se deseja registrar dados sobre conexões de clientes usando o Amazon CloudWatch Logs. Em Enable log details on client connections (Habilitar detalhes de log em conexões de cliente), siga um destes procedimentos:

   - Para ativar o log de conexão de cliente, ative Enable log details on client connections (Habilitar detalhes de log em conexões de cliente). Em Nome do grupo de CloudWatch registros de registros, selecione o nome do grupo de registros a ser usado. Em Nome do fluxo de CloudWatch registros, selecione o nome do fluxo de registros a ser usado ou deixe essa opção em branco para que possamos criar um fluxo de registros para você.
   - Para desabilitar o log de conexão de cliente, desabilite a opção Habilitar detalhes de log em conexões de cliente.

7. Em Client connect handler (Manipulador de conexão de cliente), ative Enable client connect handler (Habilitar manipulador de conexão de cliente) para ativar o manipulador de conexão de cliente. Em Client Connect Handler ARN (ARN do manipulador de conexão do cliente), especifique o nome de recurso da Amazon (ARN) da função do Lambda que contém a lógica que permite ou nega conexões.

8. Habilite ou desabilite a opção Habilitar servidores DNS. Para usar servidores DNS personalizados, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) e DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP dos servidores DNS a serem usados. Para usar o servidor DNS da VPC, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) ou DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP e adicione o endereço IP do servidor DNS da VPC.

> **Note**
>
> Verifique se os servidores DNS possam ser acessados pelos clientes.

9. Habilite ou desabilite a opção Habilitar túnel dividido. Por padrão, o túnel dividido em um endpoint da VPN está desativado.
10. Em VPC ID (ID da VPC), escolha a VPC a ser associada ao endpoint da VPN do cliente. Em Security Group IDs, escolha um ou mais dos grupos de segurança da VPC para aplicar ao endpoint do Client VPN.
11. Em VPN port (Porta VPN), selecione o número da porta VPN. O padrão é 443.
12. Para gerar um URL do portal de autoatendimento para clientes, ative Enable self-service portal (Habilitar portal de autoatendimento).
13. Em Session timeout hours (Horas do tempo limite da sessão), escolha o tempo máximo desejado de duração da sessão VPN em horas, conforme as opções disponíveis, ou deixe definido como padrão de 24 horas.
14. Em Desconectar no tempo limite da sessão, escolha se você deseja encerrar a sessão quando o tempo máximo da sessão for atingido. A escolha dessa opção exige que os usuários se reconectem manualmente ao endpoint quando a sessão expirar; caso contrário, o Client VPN tentará se reconectar automaticamente.
15. Habilite ou desabilite a opção Habilitar o banner de login do cliente. Se quiser usar o banner de login do cliente, insira o texto que será exibido em um banner nos clientes fornecidos pela AWS quando uma sessão VPN for estabelecida. Somente caracteres com codificação UTF-8. Máximo de 1400 caracteres.
16. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Modificar um endpoint da Client VPN (AWS CLI)

Use o comando modify-client-vpn-endpoint.

Excluir um AWS Client VPN endpoint

Você deverá desassociar todas as redes de destino para excluir um endpoint da VPN do cliente. Ao excluir um endpoint da Client VPN, seu estado é alterado para `deleting` e os clientes não podem mais se conectar a ele.

É possível excluir um endpoint da Client VPN usando o console ou a AWS CLI.

Para excluir um endpoint da Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, escolha Endpoints da Client VPN.
3. Escolha o endpoint da VPN do cliente a ser excluído. Escolha Actions (Ações), Delete Client VPN endpoint (Excluir endpoint da VPN do cliente).
4. Insira delete (excluir) na janela de confirmação e escolha Delete (Excluir).

Para excluir um endpoint da Client VPN (AWS CLI)

Use o comando delete-client-vpn-endpoint.

AWS Client VPN registros de conexão

É possível habilitar o registro em log de conexão para um endpoint da Client VPN, novo ou existente, e começar a capturar logs de conexão. Os logs de conexão mostram a sequência de eventos de log para o endpoint da Client VPN. Ao habilitar o registro em log de conexão, é possível especificar o nome de um stream de logs no grupo de logs. Se você não especificar um stream de logs, o serviço da Client VPN criará um para você. Em seguida, o log de conexão registra as seguintes informações: solicitações de conexão do cliente, resultados da conexão do cliente (bem-sucedidos ou malsucedidos), motivos dos resultados malsucedidos da conexão e o horário de encerramento do cliente no endpoint.

Antes de começar, você precisa ter um grupo de CloudWatch registros de registros em sua conta. Para obter mais informações, consulte Como trabalhar com grupos de registros e fluxos de registros no Guia do usuário do Amazon CloudWatch Logs. Aplicam-se cobranças pelo uso do CloudWatch Logs. Para obter mais informações, consulte os CloudWatch preços da Amazon.

Os logs de conexão da Client VPN podem ser criados usando o Amazon VPC Console ou a CLI da AWS .

Tarefas

- Habilitar o registro em log de conexão para um novo endpoint do AWS Client VPN
- Habilitar o registro em log de conexão para um endpoint do AWS Client VPN existente
- Exibir registros de AWS Client VPN conexão
- Desativar o registro de AWS Client VPN conexão

Habilitar o registro em log de conexão para um novo endpoint do AWS Client VPN

É possível habilitar o registro em log de conexão ao criar um endpoint da Client VPN usando o console ou a linha de comando.

Como habilitar o registro em log de conexão para um novo endpoint da Client VPN usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Client VPN Endpoints (Endpoints da VPN do cliente) e Create Client VPN Endpoint (Criar endpoint da VPN do cliente).
3. Conclua as opções até chegar à seção Geração de logs de conexão . Para obter mais informações sobre essas opções, consulte Crie um AWS Client VPN endpoint.
4. Em Connection logging (Log de conexão), ative Enable log details on client connections (Habilitar detalhes de log nas conexões de cliente).
5. Em Nome do grupo de CloudWatch registros de registros, escolha o nome do grupo de CloudWatch registros de registros.
6. (Opcional) Em Nome do fluxo de CloudWatch registros, escolha o nome do fluxo de CloudWatch registros.
7. Selecione Create Client VPN endpoint (Criar endpoint da VPN do cliente).

Para habilitar o registro de conexão para um novo endpoint do Client VPN usando o AWS CLI

Use o create-client-vpn-endpointcomando e especifique o `--connection-log-options` parâmetro. É possível especificar as informações de logs de conexão no formato JSON, conforme mostrado no exemplo a seguir.

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

Habilitar o registro em log de conexão para um endpoint do AWS Client VPN existente

É possível habilitar o registro em log de conexão para um endpoint da Client VPN existente usando o console ou a linha de comando.

Como habilitar o registro em log de conexão para um endpoint da Client VPN existente usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da VPN do cliente, escolha Actions (Ações) e Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).
4. Em Connection logging (Log de conexão), ative Enable log details on client connections (Habilitar detalhes de log nas conexões de cliente).
5. Em Nome do grupo de CloudWatch registros de registros, escolha o nome do grupo de CloudWatch registros de registros.
6. (Opcional) Em Nome do fluxo de CloudWatch registros, escolha o nome do fluxo de CloudWatch registros.
7. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Para habilitar o registro em log de conexão para um endpoint da Client VPN existente usando a AWS CLI

Use o comando modify-client-vpn-endpoint e especifique o parâmetro `--connection-log-options`. É possível especificar as informações de logs de conexão no formato JSON, conforme mostrado no exemplo a seguir.

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

Exibir registros de AWS Client VPN conexão

Você pode ver seus registros de conexão do Client VPN usando o console de CloudWatch registros.

Como visualizar os logs de conexão usando o console

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Grupos de logs e o grupo de log que contém seus logs de conexão.
3. Selecione o stream de logs para o endpoint da Client VPN.

> **Note**
>
> A coluna Timestamp exibe a hora em que o registro de conexão foi publicado no CloudWatch Logs, não a hora da conexão.

Para obter mais informações sobre a pesquisa de dados de log, consulte Pesquisar dados de log usando padrões de filtro no Guia do usuário do Amazon CloudWatch Logs.

Desativar o registro de AWS Client VPN conexão

É possível desativar o log de conexão de um endpoint da VPN do cliente usando o console ou a linha de comando. Quando você desativa o registro de conexão, os registros de conexão existentes nos CloudWatch Registros não são excluídos.

Como desativar o log de conexão usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da VPN do cliente, escolha Actions (Ações) e Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).
4. Em Log de conexão, desabilite a opção Habilitar detalhes de log nas conexões de cliente.
5. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Para desativar o registro de conexão usando o AWS CLI

Use o modify-client-vpn-endpointcomando e especifique o `--connection-log-options` parâmetro. Verifique se `Enabled` está definido como `false`.

AWS Client VPN exportação do arquivo de configuração do endpoint

O arquivo de configuração do AWS Client VPN endpoint é o arquivo que os clientes (usuários) usam para estabelecer uma conexão VPN com o endpoint Client VPN. Você deve baixar (exportar) esse arquivo e distribuí-lo a todos os clientes que precisam de acesso à VPN. Como alternativa, se você habilitou o portal de autoatendimento para o endpoint da Client VPN, os clientes podem fazer login no portal e baixar o arquivo de configuração. Para obter mais informações, consulte AWS Client VPN acesso ao portal de autoatendimento.

Se o endpoint da Client VPN usar a autenticação mútua, será necessário adicionar o certificado de cliente e a chave privada do cliente ao arquivo de configuração .ovpn do qual foi feito download. Depois de adicionar as informações, os clientes poderão importar o arquivo .ovpn para o software-cliente OpenVPN.

> **Important**
>
> Se você não adicionar o certificado de cliente e as informações da chave privada do cliente ao arquivo, os clientes que se autenticam usando a autenticação mútua não poderão se conectar ao endpoint da Client VPN.

Por padrão, a opção “remote-random-hostname” na configuração do cliente OpenVPN habilita o DNS curinga. Como o DNS curinga está habilitado, o cliente não armazena em cache o endereço IP do endpoint, e você não poderá executar ping no nome DNS do endpoint.

Se o endpoint da Client VPN usar a autenticação do Active Directory e se você habilitar a autenticação multifator (MFA) no diretório após distribuir o arquivo de configuração do cliente, será necessário baixar um novo arquivo e redistribuí-lo aos clientes. Os clientes não podem usar o arquivo de configuração anterior para se conectar ao endpoint da Client VPN.

Tarefas

- Exportar o arquivo de configuração do AWS Client VPN cliente
- Adicione o certificado AWS Client VPN do cliente e as principais informações para autenticação mútua

Exportar o arquivo de configuração do AWS Client VPN cliente

É possível exportar a configuração do cliente Client VPN usando o console ou o AWS CLI.

Para exportar configuração do cliente (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da Client VPN cuja configuração do cliente deve ser transferida por download e escolha Baixar a configuração do cliente.

Para exportar configuração do cliente (AWS CLI)

Use o comando export-client-vpn-client-configuration e especifique o nome do arquivo de saída.

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id
 --output text>config_filename.ovpn
```

Adicione o certificado AWS Client VPN do cliente e as principais informações para autenticação mútua

Se o endpoint da Client VPN usar a autenticação mútua, será necessário adicionar o certificado de cliente e a chave privada do cliente ao arquivo de configuração .ovpn do qual foi feito download.

Você não pode modificar o certificado de cliente ao usar a autenticação mútua.

Como adicionar o certificado de cliente e as informações de chave (autenticação mútua)

É possível usar uma das opções a seguir:

(Opção 1) Distribuir o certificado e a chave do cliente aos clientes junto com o arquivo de configuração do endpoint da Client VPN. Nesse caso, especifique o caminho para o certificado e a chave no arquivo de configuração. Abra o arquivo de configuração usando o editor de texto de sua preferência e adicione o seguinte ao final desse arquivo. */path/*Substitua pela localização do certificado e da chave do cliente (a localização é relativa ao cliente que está se conectando ao endpoint).

```
cert /path/client1.domain.tld.crt
key /path/client1.domain.tld.key
```

(Opção 2) Adicionar o conteúdo do certificado do cliente entre as tags `<cert></cert>` e o conteúdo da chave privada entre as tags `<key></key>` ao arquivo de configuração. Se você escolher essa opção, somente o arquivo de configuração será distribuído aos clientes.

Se você gerou certificados de clientes separados e chaves para cada usuário que se conectará ao endpoint da Client VPN, repita essa etapa para cada usuário.

Veja a seguir um exemplo do formato de um arquivo configuração da Client VPN que inclui o certificado e a chave do cliente.

```
client
dev tun
proto udp
remote cvpn-endpoint-0011abcabcabcabc1.prod.clientvpn.eu-west-2.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
remote-cert-tls server
cipher AES-256-GCM
verb 3

<ca>
Contents of CA
</ca>

<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>

reneg-sec 0
```

AWS Client VPN rotas

Cada AWS Client VPN endpoint tem uma tabela de rotas que descreve as rotas de rede de destino disponíveis. Cada rota na tabela de rotas determina para onde o tráfego de rede é direcionado. Você deve configurar regras de autorização para cada rota do endpoint da Client VPN para especificar quais clientes têm acesso à rede de destino.

Quando você associa uma sub-rede de uma VPC a um endpoint da Client VPN, uma rota para essa VPC é automaticamente adicionada à tabela de rotas do endpoint da Client VPN. Para permitir o acesso a redes adicionais, como redes locais com peering VPCs, a rede local (para permitir que os clientes se comuniquem entre si) ou a Internet, você deve adicionar manualmente uma rota à tabela de rotas do endpoint do Client VPN.

> **Note**
>
> Se você estiver associando várias sub-redes ao endpoint do cliente VPN, certifique-se de criar uma rota para cada sub-rede, conforme descrito aqui Solução de problemas AWS Client VPN: o acesso a uma VPC emparelhada, ao Amazon S3 ou à Internet é intermitente. Cada sub-rede associada deve ter um conjunto idêntico de rotas.

Considerações sobre o uso do túnel dividido em endpoints da Client VPN

Quando você usa túnel dividido em um endpoint da Client VPN, todas as rotas que estão nas tabelas de rotas da Client VPN são adicionadas à tabela de rotas do cliente quando a VPN é estabelecida. Se você adicionar uma rota após a VPN ser estabelecida, deverá redefinir a conexão para que a nova rota seja enviada ao cliente.

É recomendável contabilizar o número de rotas que o dispositivo cliente pode manipular antes de modificar a tabela de rotas do endpoint da Client VPN.

Tarefas

- Crie uma rota AWS Client VPN de endpoint
- Exibir AWS Client VPN rotas de endpoints
- Excluir uma rota AWS Client VPN de endpoint

Crie uma rota AWS Client VPN de endpoint

Ao criar uma rota de endpoint da Client VPN, você especifica como o tráfego da rede de destino deve ser direcionado.

Para permitir que os clientes acessem a Internet, adicione uma rota de destino `0.0.0.0/0`.

É possível adicionar rotas a um endpoint da Client VPN usando o console e a AWS CLI

Como criar uma rota de endpoint da Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da cliente VPN.
3. Selecione o endpoint da VPN do cliente ao qual você deseja adicionar a rota, escolha Route table (Tabela de rotas) e Create route (Criar rota).
4. Em Destino da rota, especifique o intervalo IPv4 CIDR para a rede de destino. Por exemplo:
   - Para adicionar uma rota para a VPC do endpoint Client VPN, insira o intervalo CIDR da VPC. IPv4
   - Para adicionar uma rota para acesso à Internet, insira `0.0.0.0/0`.
   - Para adicionar uma rota para uma VPC emparelhada, insira o intervalo CIDR da VPC emparelhada. IPv4
   - Para adicionar uma rota para uma rede local, insira o intervalo IPv4 CIDR da conexão AWS Site-to-Site VPN.
5. Em Subnet ID for target network association (ID de sub-rede da associação de rede de destino), selecione a sub-rede associada ao endpoint da VPN do cliente.

   Como alternativa, se você estiver adicionando uma rota à rede local do endpoint da VPN do cliente, selecione `local`.
6. (Opcional) Em Description (Descrição), insira uma breve descrição da rota.
7. Escolha Create route (Criar rota).

Para criar uma rota de endpoint da Client VPN (AWS CLI)

Use o comando create-client-vpn-route.

Exibir AWS Client VPN rotas de endpoints

É possível visualizar as rotas de um endpoint específico da Client VPN usando o console ou a AWS CLI.

Para visualizar rotas do endpoint da Client VPN (console)

1. No painel de navegação, escolha Endpoints da Client VPN.
2. Selecione o endpoint da VPN do cliente cujas rotas você deseja visualizar e escolha Route table (Tabela de rotas).

Para visualizar rotas do endpoint da Client VPN (AWS CLI)

Use o comando describe-client-vpn-routes.

Excluir uma rota AWS Client VPN de endpoint

É possível apenas excluir rotas da Client VPN adicionadas manualmente. Não é possível excluir rotas que foram adicionadas automaticamente quando você associou uma sub-rede ao endpoint da Client VPN. Para excluir rotas que foram adicionadas automaticamente, você deve desassociar a sub-rede que iniciou sua criação do endpoint da Client VPN.

É possível excluir uma rota de um endpoint da Client VPN usando o console ou a AWS CLI.

Como excluir uma rota de endpoint da Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da VPN do cliente do qual deseja excluir a rota e escolha Route table (Tabela de rotas).
4. Selecione a rota a ser excluída, escolha Delete route (Excluir rota) e Delete route (Excluir rota).

Para excluir uma rota de endpoint da Client VPN (AWS CLI)

Use o comando delete-client-vpn-route.

AWS Client VPN redes alvo

Uma rede de destino é uma sub-rede em uma VPC. Um AWS Client VPN endpoint deve ter pelo menos uma rede de destino para permitir que os clientes se conectem a ele e estabeleçam uma conexão VPN.

Para obter mais informações sobre os tipos de acesso que você pode configurar (como permitir que os clientes acessem a Internet), consulte Cenários e exemplos da Client VPN.

Requisitos de rede de destino da Client VPN

Ao criar uma rede de destino, as seguintes regras se aplicam:

- A sub-rede deve ter um bloco CIDR com pelo menos uma máscara de bits /27, por exemplo 10.0.0.0/27. A sub-rede também deve ter sempre 20 endereços IP disponíveis, pelo menos.

- O bloco CIDR da sub-rede não pode se sobrepor ao intervalo CIDR cliente do endpoint da Client VPN.
- Se você associar mais de uma sub-rede a um endpoint da Client VPN, cada sub-rede deverá estar em uma zona de disponibilidade diferente. Recomendamos que você associe pelo menos duas sub-redes para fornecer redundância de zona de disponibilidade.
- Se você especificou uma VPC ao criar o endpoint da Client VPN, a sub-rede deverá estar na mesma VPC. Se você ainda não associou uma VPC ao endpoint da Client VPN, poderá escolher qualquer sub-rede em qualquer VPC.

  Todas as associações de sub-rede adicionais devem ser na mesma VPC. Para associar uma sub-rede de uma VPC diferente, primeiro você deve modificar o endpoint da Client VPN e alterar a VPC associada a ele. Para obter mais informações, consulte Modificar um AWS Client VPN endpoint.

Quando você associa uma sub-rede a um endpoint da Client VPN, nós adicionamos automaticamente a rota local da VPC na qual a sub-rede associada está provisionada à tabela de rotas do endpoint da Client VPN.

> **Note**
>
> Depois que suas redes de destino forem associadas, ao adicionar ou remover outras CIDRs à sua VPC conectada, você deverá realizar uma das seguintes operações para atualizar a rota local da tabela de rotas do endpoint do Client VPN:
>
> - Desassocie o endpoint da Client VPN da rede de destino e, em seguida, associe-o novamente.
> - Adicione manualmente a rota ou remova-a da tabela de rotas do endpoint da Client VPN.

Depois de associar a primeira sub-rede ao endpoint da Client VPN, o status do endpoint da Client VPN muda de `pending-associate` para `available`, e os clientes podem estabelecer uma conexão VPN.

Tarefas

- Associar uma rede de destino a um endpoint do AWS Client VPN
- Aplicar um grupo de segurança a uma rede de destino no AWS Client VPN
- Exibir redes de AWS Client VPN destino

- Desassociar uma rede de destino de um endpoint do AWS Client VPN

Associar uma rede de destino a um endpoint do AWS Client VPN

Você pode associar uma ou mais redes de destino (sub-redes) a um endpoint Client VPN usando o console Amazon VPC ou a CLI. AWS Antes de associar uma rede de destino a um endpoint da Client VPN, familiarize-se com os requisitos. Consulte Requisitos para criar uma rede de destino.

Como associar uma rede de destino a um endpoint da Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint de VPN do cliente ao qual deseja associar a rede de destino, escolha Target network associations (Associações da rede de destino) e Associate target network (Associar rede de destino).
4. Para VPC, selecione a VPC na qual a sub-rede está localizada. Se você especificou uma VPC ao criar o endpoint da Client VPN ou se tiver associações de sub-rede anteriores, ela deverá ser a mesma VPC.
5. Em Choose a subnet to associate (Escolher uma sub-rede para associar), escolha a sub-rede a ser associada ao endpoint da VPN do cliente.
6. SelecioneAssociate target network (Associar rede de destino).

Para associar uma rede de destino a um endpoint da Client VPN (AWS CLI)

Use o comando associate-client-vpn-target-network.

Aplicar um grupo de segurança a uma rede de destino no AWS Client VPN

Ao criar um endpoint da Client VPN, você pode especificar os grupos de segurança a serem aplicados à rede de destino. Quando você associa a primeira rede de destino a um endpoint da Client VPN, aplicamos automaticamente o grupo de segurança padrão da VPC na qual a sub-rede associada está localizada. Para obter mais informações, consulte Grupos de segurança.

É possível alterar os grupos de segurança para o endpoint da Client VPN. As regras de grupo de segurança de que você precisa dependem do tipo de acesso VPN que você deseja configurar. Para obter mais informações, consulte Cenários e exemplos da Client VPN.

Para aplicar um grupo de segurança a uma rede de destino (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da Client VPN ao qual aplicar os grupos de segurança.
4. Escolha Security Groups (Grupos de segurança) e Apply Security Groups (Aplicar grupos de segurança).
5. Selecione o (s) grupo (s) de segurança apropriado (s) em Grupo de segurança IDs.
6. Escolha Apply Security Groups (Aplicar grupos de segurança).

Para aplicar um grupo de segurança a uma rede de destino (AWS CLI)

Use o client-vpn-target-network comando apply-security-groups-to-.

Exibir redes de AWS Client VPN destino

É possível visualizar os destinos associados a um endpoint da Client VPN usando o console ou a AWS CLI.

Para visualizar redes de destino (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint de VPN do cliente apropriado e escolha Target network associations (Associações da rede de destino).

Para visualizar as redes de destino usando o AWS CLI

Use o comando describe-client-vpn-target-networks.

Desassociar uma rede de destino de um endpoint do AWS Client VPN

Quando você desassocia uma rede de destino, todas as rotas que foram adicionadas manualmente à tabela de rotas do endpoint da Client VPN são excluídas, bem como a rota que foi criada automaticamente quando a associação de rede de destino foi feita (a rota local da VPC). Se você desassociar todas as redes de destino de um endpoint da Client VPN, os clientes não poderão mais estabelecer uma conexão VPN.

Como desassociar uma rede de destino de um endpoint da Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint de VPN do cliente ao qual a rede de destino está associada e escolha Target network associations (Associações da rede de destino).
4. Selecione a rede de destino a ser desassociada, escolha Disassociate (Desassociar) e Disassociate target network (Desassociar rede de destino).

Para desassociar uma rede de destino de um endpoint da Client VPN (AWS CLI)

Use o comando disassociate-client-vpn-target-network.

AWS Client VPN tempo limite máximo de duração da sessão de VPN

AWS Client VPN fornece várias opções para a duração máxima da sessão de VPN, que é o tempo máximo permitido para uma conexão do cliente com o endpoint do Client VPN. É possível configurar uma duração máxima de sessão VPN menor para ajudar a atender aos requisitos de segurança e conformidade. Por padrão, a duração máxima da sessão VPN é 24 horas. Depois de definir a duração máxima da sessão, você pode controlar o que acontece com essa sessão quando o tempo limite é atingido. A opção de desconexão no tempo limite da sessão permite que você encerre a sessão ou tente automaticamente uma reconexão com o endpoint. O encerramento de uma sessão permite que você tenha mais controle sobre a segurança do endpoint ao impor a duração máxima da sessão de VPN. Se uma sessão for definida para terminar quando o tempo máximo for atingido, os usuários precisarão se reconectar e fornecer suas credenciais de autenticação para restabelecer a conexão VPN.

Quando a desconexão na sessão, o tempo limite é definido para se reconectar automaticamente e o tempo máximo da sessão é atingido,

- uma nova sessão é estabelecida automaticamente no caso de credenciais de usuário em cache (Active Directory) ou autenticação baseada em certificado (Autenticação mútua). Para se desconectar totalmente e não se reconectar automaticamente, esses usuários devem se desconectar manualmente.

- uma nova sessão não é estabelecida automaticamente no caso da autenticação federada (SAML). Esses usuários devem se autenticar novamente após a expiração do tempo limite da sessão para restabelecer a conexão VPN.

> **Note**
>
> - Quando o valor máximo da duração da sessão de VPN é reduzido em relação ao valor atual, todas as sessões ativas de VPN conectadas ao endpoint por um período maior do que a duração recém-definida são desconectadas.
> - Alterar a opção de desconexão no tempo limite da sessão aplica a nova configuração a todas as sessões abertas no momento.

Configurar a sessão máxima de VPN durante a criação de um AWS Client VPN endpoint

Duração da sessão VPN é configurada durante a criação de um endpoint da Client VPN. Consulte Crie um AWS Client VPN endpoint para obter as etapas para criar um endpoint da Client VPN e definir a duração máxima da sessão.

Tarefas

- Exibir a duração máxima AWS Client VPN atual da sessão de VPN
- Modifique a duração máxima AWS Client VPN da sessão e o comportamento do tempo limite

Exibir a duração máxima AWS Client VPN atual da sessão de VPN

Use as etapas a seguir para visualizar a duração máxima atual da sessão VPN da Client VPN.

Visualizar a duração máxima da sessão do cliente VPN para um endpoint da Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints da Client VPN.
3. Selecione o endpoint da Client VPN que deseja visualizar.
4. Verifique se a guia Details (Detalhes) está selecionada.

5. Veja a duração máxima atual da sessão de VPN ao lado de Horas de tempo limite da sessão e se a opção Desconectar no tempo limite está ativada ou desativada.

Veja a duração máxima da sessão do cliente VPN atual para um endpoint do cliente VPN (AWS CLI)

Use o comando describe-client-vpn-endpoints.

Modifique a duração máxima AWS Client VPN da sessão e o comportamento do tempo limite

Use as etapas a seguir para modificar a duração máxima de uma sessão VPN existente do Client VPN e alterar o comportamento de desconexão no tempo limite da sessão.

Modificar uma duração máxima de sessão do cliente VPN existente para um endpoint da Client VPN (console)

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN endpoints (Endpoints da VPN do cliente).
3. Selecione o endpoint do cliente VPN que deseja modificar, escolha Actions (Ações) e escolha Modify Client VPN Endpoint (Modificar endpoint do cliente VPN).
4. Na sessão Session timeout hours (Horas do tempo limite da sessão), escolha o tempo máximo desejado de duração de sessão VPN em horas.
5. Em Desconectar no tempo limite da sessão, escolha se você deseja desconectar uma sessão quando o tempo limite máximo da sessão for atingido. Por padrão, isso é desativado na primeira vez que você modifica um endpoint.
6. Escolha Modify Client VPN endpoint (Modificar endpoint da VPN do cliente).

Modificar uma duração máxima de sessão VPN existente para um endpoint do cliente VPN (AWS CLI)

Use o comando modify-client-vpn-endpoint.

Segurança em AWS Client VPN

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam AWS Client VPN, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

AWS Client VPN faz parte do serviço Amazon VPC. Para obter mais informações sobre segurança na Amazon VPC, consulte Segurança no Guia do usuário da Amazon VPC.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar a Client VPN. Os tópicos a seguir mostram como configurar a Client VPN para atender aos seus objetivos de segurança e de conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos de Client VPN.

Tópicos

- Proteção de dados em AWS Client VPN
- Gerenciamento de identidade e acesso para AWS Client VPN
- Resiliência em AWS Client VPN
- Segurança da infraestrutura em AWS Client VPN
- Práticas recomendadas de segurança para AWS Client VPN
- IPv6 considerações para AWS Client VPN

Proteção de dados em AWS Client VPN

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados no AWS Client VPN. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Client VPN ou outro Serviços da AWS usando o console AWS CLI, a API ou AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato

livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia em trânsito

AWS Client VPN fornece conexões seguras de qualquer local usando o Transport Layer Security (TLS) 1.2 ou posterior.

Privacidade do tráfego entre redes

Habilitar o acesso entre redes

É possível permitir que os clientes se conectem à sua VPC e outras redes por meio de um endpoint da VPN do Cliente Para obter mais informações e exemplos, consulte Cenários e exemplos da Client VPN.

Restringir o acesso a redes

É possível configurar seu endpoint da VPN do Cliente para restringir o acesso a recursos específicos em sua VPC. Para autenticação baseada no usuário, você também pode restringir o acesso a partes da rede, com base no grupo de usuários que acessa o endpoint do VPN do Cliente Para obter mais informações, consulte Restrição do acesso à rede usando o Client VPN.

Autenticar clientes

A autenticação é implementada no primeiro ponto de entrada na Nuvem AWS . Ela é usada para determinar se os clientes têm permissão para se conectar ao endpoint da cliente VPN. Se a autenticação for bem-sucedida, os clientes se conectarão ao endpoint da cliente VPN e estabelecerão uma sessão de VPN. Se a autenticação falhar, a conexão será negada, e o cliente será impedido de estabelecer uma sessão de VPN.

O VPN do Cliente oferece os seguintes tipos de autenticação de cliente:

- Autenticação do Active Directory (baseada no usuário)
- Autenticação mútua (baseada em certificado)
- Single Sign-On (autenticação federada baseada em SAML) (baseado no usuário)

Gerenciamento de identidade e acesso para AWS Client VPN

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar os recursos da Client VPN. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticação com identidades
- Gerenciar o acesso usando políticas
- Como AWS Client VPN funciona com o IAM
- Exemplos de políticas baseadas em identidade para o AWS Client VPN
- Solução de problemas AWS Client VPN de identidade e acesso
- Usando funções vinculadas a serviços para AWS Client VPN

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Client VPN.

Usuário do serviço: se você usar o serviço da Client VPN para fazer o trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que usar mais recursos da Client VPN para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador. Se não for possível acessar um recurso na Client VPN, consulte Solução de problemas AWS Client VPN de identidade e acesso.

Administrador do serviço: se você for o responsável pelos recursos da Client VPN na empresa, provavelmente terá acesso total à Client VPN. Cabe a você determinar quais funcionalidades e recursos da Client VPN os usuários do serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com a Client VPN, consulte Como AWS Client VPN funciona com o IAM.

Administrador do IAM: se você for administrador do IAM, talvez queira saber detalhes sobre como pode escrever políticas para gerenciar o acesso à Client VPN. Para visualizar exemplos de políticas baseadas em identidade da VPN que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o AWS Client VPN.

Autenticação com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator da AWS no IAM no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a

conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, é recomendável usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Guia do Usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode alternar de um usuário para uma função do IAM (console). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Guia do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso

usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.

- Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.
- Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados a serviço.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida

ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal

especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.

- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como AWS Client VPN funciona com o IAM

Antes de usar o IAM para gerenciar o acesso à Client VPN, saiba quais recursos do IAM estão disponíveis para uso com à Client VPN.

Recursos do IAM que você pode usar com o AWS Client VPN

Recurso do IAM	Compatibilidade com Client VPN
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim

Recurso do IAM	Compatibilidade com Client VPN
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim
Perfis vinculados a serviço	Sim

Políticas baseadas em identidade para a Client VPN

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para a Client VPN

Para visualizar exemplos de políticas baseadas em identidade da Client VPN, consulte Exemplos de políticas baseadas em identidade para o AWS Client VPN.

Políticas baseadas em recursos na Client VPN

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações de políticas para a Client VPN

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do Client VPN, consulte Ações definidas pelo AWS Client VPN na Referência de Autorização do Serviço.

As ações de políticas na Client VPN usam o seguinte prefixo antes da ação:

```
ec2
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

Para visualizar exemplos de políticas baseadas em identidade da Client VPN, consulte Exemplos de políticas baseadas em identidade para o AWS Client VPN.

Recursos de políticas para a Client VPN

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do Client VPN e seus ARNs, consulte Recursos definidos pelo AWS Client VPN na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo AWS Client VPN.

Para visualizar exemplos de políticas baseadas em identidade da Client VPN, consulte Exemplos de políticas baseadas em identidade para o AWS Client VPN.

Chaves de condição de políticas para a Client VPN

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do Client VPN, consulte Chaves de condição AWS do Client VPN na Referência de Autorização do Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo AWS Client VPN.

Para visualizar exemplos de políticas baseadas em identidade da Client VPN, consulte Exemplos de políticas baseadas em identidade para o AWS Client VPN.

ACLs em Client VPN

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com a Client VPN

Compatível com ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usar credenciais temporárias com a Client VPN

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil do IAM (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões de entidade principal entre serviços para a Client VPN

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Perfis de serviço para a Client VPN

Compatível com perfis de serviço: sim

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

Perfis vinculados a serviços para a Client VPN

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados a serviço.

Exemplos de políticas baseadas em identidade para o AWS Client VPN

Por padrão, os usuários e os perfis não têm permissão para criar ou modificar recursos da Client VPN. Eles também não podem realizar tarefas usando a AWS API AWS Management Console,

AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo Client VPN, incluindo o formato do ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para AWS Client VPN na Referência de Autorização de Serviço.

Tópicos

- Práticas recomendadas de política
- Permitir que os usuários visualizem suas próprias permissões

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos da Client VPN em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas

usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.

- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
```

```
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solução de problemas AWS Client VPN de identidade e acesso

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com a Client VPN e o IAM.

Tópicos

- Não tenho autorização para executar uma ação na Client VPN
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos de Client VPN

Não tenho autorização para executar uma ação na Client VPN

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `ec2:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `ec2:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, suas políticas deverão ser atualizadas para permitir que você passe um perfil para a Client VPN.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação na Client VPN. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos de Client VPN

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se a Client VPN é compatível com esses recursos, consulte Como AWS Client VPN funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Usando funções vinculadas a serviços para AWS Client VPN

AWS Client VPN usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Um perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente à Client VPN. As funções vinculadas ao serviço são predefinidas pelo Client VPN e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Tópicos

- Usando funções para AWS Client VPN
- Usar perfis para autorização de conexão da Client VPN;

Usando funções para AWS Client VPN

AWS Client VPN usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Um perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente à Client VPN. As funções vinculadas ao serviço são predefinidas pelo Client VPN e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Um perfil vinculado ao serviço facilita a configuração da Client VPN porque você não precisa adicionar as permissões necessárias manualmente. A Client VPN define as permissões de seus perfis vinculadas ao serviço e, exceto se definido de outra forma, somente a Client VPN pode

assumir seus perfis. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege seus recursos da Client VPN, pois você não pode remover por engano as permissões para acessar os recursos.

Permissões de função vinculada ao serviço para a Client VPN

O Client VPN usa a função vinculada ao serviço chamada AWSServiceRoleForClientVPN — Allow Client VPN para criar e gerenciar recursos relacionados às suas conexões VPN.

A função vinculada ao serviço AWSServiceRoleForClientVPN confia no seguinte serviço para assumir a função:

- `clientvpn.amazonaws.com`

Essa função vinculada ao serviço usa a política gerenciada Client. VPNService RolePolicy Para ver as permissões dessa política, consulte Cliente VPNService RolePolicy na Referência de política AWS gerenciada.

Crie uma função vinculada ao serviço para o Client VPN

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria o primeiro endpoint de Client VPN em sua conta com a AWS Management Console, a ou a AWS API AWS CLI, a Client VPN cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria o primeiro endpoint da Client VPN em sua conta, a Client VPN cria o perfil vinculado ao serviço para você novamente.

Editar uma função vinculada ao serviço para Client VPN

O Client VPN não permite que você edite a função vinculada ao serviço AWSService RoleForClient VPN. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma descrição de perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para Client VPN

Se você não precisar mais usar o Client VPN, recomendamos que você exclua a função vinculada ao serviço AWSServiceRoleForClientVPN.

Você deve primeiro excluir os recursos da Client VPN relacionados. Isso garante que você não remova por engano a permissão para acessar os recursos.

Use o console, a CLI ou a API do IAM para excluir funções vinculadas ao serviço. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Usar perfis para autorização de conexão da Client VPN;

AWS Client VPN usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Um perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente à Client VPN. As funções vinculadas ao serviço são predefinidas pelo Client VPN e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Um perfil vinculado ao serviço facilita a configuração da Client VPN porque você não precisa adicionar as permissões necessárias manualmente. A Client VPN define as permissões de seus perfis vinculadas ao serviço e, exceto se definido de outra forma, somente a Client VPN pode assumir seus perfis. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege seus recursos da Client VPN, pois você não pode remover por engano as permissões para acessar os recursos.

Permissões de função vinculada ao serviço para a Client VPN

O Client VPN usa a função vinculada ao serviço chamada AWSServiceRoleForClientVPNConnections— Função vinculada ao serviço para conexões VPN do cliente.

A função AWSService RoleForClient VPNConnections vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `clientvpn-connections.amazonaws.com`

A política de permissões de função chamada Client VPNService ConnectionsRolePolicy permite que o Client VPN conclua as seguintes ações nos recursos especificados:

- Ação: `lambda:InvokeFunction` em `arn:aws:lambda:*:*:function:AWSClientVPN-*`

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Crie uma função vinculada ao serviço para o Client VPN

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria o primeiro endpoint de Client VPN em sua conta com a AWS Management Console, a ou a AWS API AWS CLI, a Client VPN cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria o primeiro endpoint da Client VPN em sua conta, a Client VPN cria o perfil vinculado ao serviço para você novamente.

Editar uma função vinculada ao serviço para Client VPN

O Client VPN não permite que você edite a função AWSService RoleForClient VPNConnections vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma descrição de perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para Client VPN

Se você não precisar mais usar o Client VPN, recomendamos que você exclua a função AWSServiceRoleForClientVPNConnectionsvinculada ao serviço.

Você deve primeiro excluir os recursos da Client VPN relacionados. Isso garante que você não remova por engano a permissão para acessar os recursos.

Use o console, a CLI ou a API do IAM para excluir funções vinculadas ao serviço. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Resiliência em AWS Client VPN

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas

de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, AWS Client VPN oferece recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Várias redes de destino para alta disponibilidade

Associe uma rede de destino a um endpoint da Client VPN para permitir que os clientes estabeleçam sessões VPN. As redes de destino são sub-redes em sua VPC. Cada sub-rede que você associa ao endpoint da Client VPN deve pertencer a uma zona de disponibilidade diferente. É possível associar várias sub-redes a um endpoint da Client VPN para alta disponibilidade.

Segurança da infraestrutura em AWS Client VPN

Como um serviço gerenciado, AWS o Client VPN é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Client VPN pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Práticas recomendadas de segurança para AWS Client VPN

AWS Client VPN fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As práticas recomendadas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

Regras de autorização

Use regras de autorização para restringir quais usuários podem acessar sua rede. Para obter mais informações, consulte Regras de autorização.

Grupos de segurança

Use grupos de segurança para controlar quais recursos os usuários podem acessar em sua VPC. Para obter mais informações, consulte Grupos de segurança.

Listas de revogação de certificados de cliente

Use listas de revogação de certificados de cliente para revogar o acesso a um endpoint da Client VPN para certificados de cliente específicos. Por exemplo, quando um usuário sai da sua organização. Para obter mais informações, consulte Listas de revogação de certificados de cliente.

Desconectar no tempo limite da sessão

Desconecte uma sessão quando o tempo máximo da sessão Client VPN for atingido, impondo uma duração máxima de sessão de VPN. Para obter mais informações, consulte Duração máxima da sessão VPN .

Ferramentas de monitoramento

Use ferramentas de monitoramento para controlar a disponibilidade e o desempenho de seus endpoints da Client VPN. Para obter mais informações, consulte Monitorar a Client VPN.

Gerenciamento de identidade e acesso

Gerencie o acesso aos recursos do Client VPN APIs usando políticas do IAM para seus usuários e funções do IAM. Para obter mais informações, consulte Gerenciamento de identidade e acesso para AWS Client VPN.

IPv6 considerações para AWS Client VPN

Atualmente, o serviço Client VPN não oferece suporte ao roteamento de IPv6 tráfego pelo túnel VPN. No entanto, há casos em que o IPv6 tráfego deve ser roteado para o túnel VPN para evitar IPv6 vazamentos. IPv6 O vazamento pode ocorrer quando ambos IPv4 IPv6 estão habilitados e conectados à VPN, mas a VPN não direciona o IPv6 tráfego para seu túnel. Nesse caso, ao se conectar a um destino IPv6 habilitado, você ainda está se conectando com o IPv6 endereço fornecido pelo seu ISP. Isso vazará seu IPv6 endereço real. As instruções abaixo explicam como rotear o IPv6 tráfego para o túnel VPN.

As seguintes diretivas IPv6 relacionadas devem ser adicionadas ao seu arquivo de configuração do Client VPN para evitar IPv6 vazamentos:

```
ifconfig-ipv6 arg0 arg1
route-ipv6 arg0
```

Um exemplo pode ser:

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/4
```

Neste exemplo, `ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1` definirá o endereço do dispositivo de túnel local como sendo `fd15:53b6:dead::2` e o IPv6 endereço do endpoint IPv6 VPN remoto como sendo`fd15:53b6:dead::1`.

O próximo comando `route-ipv6 2000::/4` roteará IPv6 os endereços de `2000:0000:0000:0000:0000:0000:0000:0000` para `2fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` dentro da conexão VPN.

> **Note**
>
> Para o roteamento do dispositivo “TAP” no Windows, por exemplo, o segundo parâmetro de `ifconfig-ipv6` será usado como destino de rota para `--route-ipv6`.

As próprias organizações devem configurar os dois parâmetros de `ifconfig-ipv6` e podem usar endereços em `100::/64` (de`0100:0000:0000:0000:0000:0000:0000:0000` a `0100:0000:0000:0000:ffff:ffff:ffff:ffff`) ou `fc00::/7` (de

`fc00:0000:0000:0000:0000:0000:0000:0000` a `fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`). `100::/64` é um bloco de endereços somente para descarte e `fc00::/7` é exclusivo no local.

Outro exemplo:

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/3
route-ipv6 fc00::/7
```

Neste exemplo, a configuração roteará todo o IPv6 tráfego atualmente alocado para a conexão VPN.

Verificação

Provavelmente, sua organização terá os próprios testes. Uma verificação básica é configurar uma conexão VPN de túnel completo e, em seguida, executar o ping6 em um IPv6 servidor usando o IPv6 endereço. O IPv6 endereço do servidor deve estar no intervalo especificado pelo `route-ipv6` comando. Esse teste de ping deve falhar. No entanto, isso pode mudar se o IPv6 suporte for adicionado ao serviço Client VPN no futuro. Se o ping for bem-sucedido e você conseguir acessar sites públicos quando conectado no modo de túnel completo, talvez seja necessário fazer mais uma solução de problemas. Também existem algumas ferramentas disponíveis publicamente.

Monitoramento AWS Client VPN

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS Client VPN suas outras AWS soluções. É possível usar os recursos a seguir para monitorar seus endpoints de Client VPN, analisar padrões de tráfego e solucionar problemas com os endpoints de Client VPN.

Amazon CloudWatch

Monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. Você pode coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas EC2 instâncias da Amazon e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

AWS CloudTrail

Captura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Todas as ações do Client VPN são registradas CloudTrail e documentadas na Amazon EC2 API Reference.

CloudWatch Registros da Amazon

Permite monitorar as tentativas de conexão feitas a seu endpoint AWS Client VPN . É possível exibir as tentativas de conexão e as redefinições de conexão para as conexões da Client VPN. É possível ver as tentativas de conexão bem-sucedidas e com falha. Você pode especificar o stream de CloudWatch registros de registros para registrar os detalhes da conexão. Para obter mais informações, consulte Registro de conexão para um AWS Client VPN endpoint o Guia do usuário do Amazon CloudWatch Logs.

Tópicos

- CloudWatch Métricas da Amazon para AWS Client VPN

CloudWatch Métricas da Amazon para AWS Client VPN

AWS Client VPN publica as seguintes métricas na Amazon CloudWatch para seus endpoints Client VPN. As métricas são publicadas na Amazon CloudWatch a cada cinco minutos.

Métrica	Descrição
ActiveConnectionsCount	O número de conexões ativas ao endpoint da Client VPN. Unidades: contagem
AuthenticationFailures	O número de falhas de autenticação para o endpoint da Client VPN. Unidades: contagem
CrlDaysToExpiry	O número de dias até a Lista de revogação de certificados (CRL) configurada no endpoint da Client VPN expirar. Unidades: dias
EgressBytes	Número de bytes enviados do endpoint da Client VPN. Unidades: bytes
EgressPackets	Número de pacotes enviados do endpoint da Client VPN. Unidades: contagem
IngressBytes	O número de bytes recebidos pelo endpoint da Client VPN. Unidades: bytes
IngressPackets	O número de pacotes recebidos pelo endpoint da Client VPN.

Métrica	Descrição
	Unidades: contagem
SelfServicePortalClientConfigurationDownloads	O número de downloads do arquivo de configuração do endpoint da Client VPN do portal de autoatendimento. Unidade: contagem

AWS Client VPN publica as seguintes métricas de avaliação de postura para seus endpoints do Client VPN.

Métrica	Descrição
ClientConnectHandlerTimeouts	O número de tempos limite ao chamar o gerenciador de conexão do cliente para conexões com o endpoint da VPN do Cliente. Unidades: contagem
ClientConnectHandlerInvalidResponses	O número de respostas inválidas devolvidas pelo gerenciador de conexão do cliente para conexões com o endpoint da VPN do Cliente. Unidades: contagem
ClientConnectHandlerOtherExecutionErrors	O número de erros inesperados ao executar o gerenciador de conexão do cliente para conexões com o endpoint da VPN do Cliente. Unidades: contagem
ClientConnectHandlerThrottlingErrors	O número de erros de controle de utilização ao chamar o gerenciador de conexão do cliente para conexões com o endpoint da Client VPN. Unidades: contagem

Métrica	Descrição
ClientConnectHandlerDeniedConnections	O número de conexões negadas pelo gerenciador de conexão do cliente para conexões com o endpoint da VPN do Cliente. Unidades: contagem
ClientConnectHandlerFailedServiceErrors	O número de erros colaterais no serviço ao executar o gerenciador de conexão do cliente para conexões com o endpoint da VPN do Cliente. Unidades: contagem

É possível filtrar as métricas de seu endpoint da Client VPN por endpoint.

CloudWatch permite que você recupere estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Considere uma métrica como uma variável a ser monitorada, e os pontos de dados como os valores dessa variável ao longo do tempo. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

É possível usar métricas para verificar se o sistema está executando conforme o esperado. Por exemplo, você pode criar um CloudWatch alarme para monitorar uma métrica específica e iniciar uma ação (como enviar uma notificação para um endereço de e-mail) se a métrica estiver fora do que você considera um intervalo aceitável.

Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

Tarefas

- Veja as métricas de endpoint do Client VPN na Amazon CloudWatch

Veja as métricas de endpoint do Client VPN na Amazon CloudWatch

É possível ver as métricas do endpoint do seu Client VPN da maneira a seguir.

Para visualizar métricas usando o CloudWatch console

As métricas são agrupadas primeiro pelo namespace do serviço e, em seguida, por várias combinações de dimensão dentro de cada namespace.

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Métricas.
3. Em All metrics (Todas as métricas), escolha o namespace da métrica ClientVPN (VPN do Cliente).
4. Para visualizar as métricas, selecione a dimensão da métrica by endpoint (por endpoint).

Para visualizar métricas usando o AWS CLI

Em um prompt de comando, use o comando a seguir para listar as métricas que estão disponíveis para a VPN do Cliente.

```
aws cloudwatch list-metrics --namespace "AWS/ClientVPN"
```

AWS Client VPN cotas

Sua AWS conta tem as seguintes cotas, anteriormente chamadas de limites, relacionadas aos endpoints do Client VPN. A menos que especificado de outra forma, cada cota é específica da região . Você pode solicitar o aumento de algumas cotas, porém, algumas delas não podem ser aumentadas.

Para solicitar o aumento da cota para uma cota ajustável, selecione Yes (Sim) na coluna Adjustable (Ajustável). Para obter mais informações, consulte Solicitar um aumento da cota no Guia do usuário do Service Quotas.

Cotas da Client VPN

Nome	Padrão	Ajustável
Regras de autorização por endpoint da Client VPN	200	Sim
Endpoints da Client VPN por região	5	Sim
Conexões de cliente simultâneas por endpoint de cliente VPN	Esse valor depende do número de associações de sub-rede por endpoint. • 1 a 7.000 • 2 a 36.500 • 3 a 66.500 • 4 a 96.500 • 5 a 126.000	Sim
Operações simultâneas por endpoint do cliente VPN †	10	Não
Entradas em uma lista de revogação de certificados de cliente para endpoints do cliente VPN	20.000	Não

Nome	Padrão	Ajustável
Rotas por associação de rede de destino do Client VPN	100	Sim

† As operações incluem:

- Associar ou desassociar sub-redes
- Criar ou excluir grupos de segurança

Cotas de usuários e grupos

Ao configurar usuários e grupos para o Active Directory ou para um IdP baseado em SAML, as seguintes cotas se aplicam:

- Os usuários podem pertencer a, no máximo, 200 grupos. Todos os grupos após o 200º grupo são ignorados.
- O tamanho máximo do ID do grupo é 255 caracteres.
- O tamanho máximo do ID do nome é 255 caracteres. Os caracteres após o 255º caractere são truncados.

Considerações gerais

Leve o seguinte em consideração ao usar endpoints da Client VPN:

- Se você usa o Active Directory para autenticar o usuário, o endpoint do Client VPN deve pertencer à mesma conta do AWS Directory Service recurso usado para autenticação do Active Directory.
- Se você usar a autenticação federada baseada em SAML para autenticar um usuário, o endpoint do Client VPN deverá pertencer à mesma conta do provedor de identidade SAML do IAM que você criou para definir a relação entre IdP e confiança. AWS O provedor de identidade SAML do IAM pode ser compartilhado entre vários endpoints do Client VPN na mesma AWS conta.

Solução de problemas AWS Client VPN

As seções a seguir pode ajudar a solucionar problemas que possam surgir com um endpoint da Client VPN.

Para obter mais informações sobre a solução de problemas de software baseado em OpenVPN que os clientes usam para se conectar a um cliente VPN, consulte Solução de problemas de conexão do cliente VPN no Guia do usuário do AWS Client VPN .

Problemas comuns

- Solução de problemas AWS Client VPN: Não foi possível resolver o nome DNS do endpoint do Client VPN
- Solução de problemas AWS Client VPN: o tráfego não está sendo dividido entre sub-redes
- Solução de problemas AWS Client VPN: as regras de autorização para grupos do Active Directory não funcionam conforme o esperado
- Solução de problemas AWS Client VPN: os clientes não conseguem acessar uma VPC emparelhada, o Amazon S3 ou a Internet
- Solução de problemas AWS Client VPN: o acesso a uma VPC emparelhada, ao Amazon S3 ou à Internet é intermitente
- Solução de problemas AWS Client VPN: o software cliente retorna um erro de TLS ao tentar se conectar ao Client VPN
- Solução de problemas AWS Client VPN: o software cliente retorna erros de nome de usuário e senha — autenticação do Active Directory
- Solução de problemas AWS Client VPN: o software cliente retorna erros de nome de usuário e senha — autenticação federada
- Solução de problemas AWS Client VPN: os clientes não conseguem se conectar — autenticação mútua
- Solução de problemas AWS Client VPN: o cliente retorna um erro de credenciais que excedem o tamanho máximo no Client VPN — autenticação federada
- Solução de problemas AWS Client VPN: o cliente não abre o navegador para um endpoint — autenticação federada
- Solução de problemas AWS Client VPN: o cliente retorna erro sem portas disponíveis — autenticação federada

- Solução de problemas AWS Client VPN: uma conexão é encerrada devido a uma incompatibilidade de IP
- Solução de problemas AWS Client VPN: o tráfego de roteamento para a LAN não está funcionando conforme o esperado
- Solução de problemas AWS Client VPN: verifique o limite de largura de banda para um endpoint Client VPN
- Solução de problemas AWS Client VPN: problemas de conectividade de túnel com uma VPC

Solução de problemas AWS Client VPN: Não foi possível resolver o nome DNS do endpoint do Client VPN

Problema

Não consigo resolver o nome DNS do endpoint da Client VPN.

Causa

O arquivo de configuração do endpoint da Client VPN inclui um parâmetro chamado `remote-random-hostname`. Esse parâmetro força o cliente a preceder o nome DNS com uma string aleatória para impedir o armazenamento em cache de DNS. Alguns clientes não reconhecem esse parâmetro e, portanto, não precedem o nome DNS com a string aleatória necessária.

Solução

Abra o arquivo de configuração do endpoint da Client VPN usando seu editor de texto preferido. Localize a linha que especifica o nome DNS do endpoint do Client VPN e acrescente uma string aleatória a ela para que o formato seja. *`random_string.displayed_DNS_name`* Por exemplo:

- Nome DNS original: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- Nome DNS modificado: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

Solução de problemas AWS Client VPN: o tráfego não está sendo dividido entre sub-redes

Problema

Estou tentando dividir o tráfego de rede entre duas sub-redes. O tráfego privado deve ser roteado por uma sub-rede privada, enquanto o tráfego da Internet deve ser roteado por uma sub-rede pública. No entanto, somente uma rota está sendo usada, embora eu tenha adicionado ambas as rotas à tabela de rotas do endpoint da Client VPN.

Causa

É possível associar várias sub-redes a um endpoint da Client VPN, mas somente uma sub-rede por zona de disponibilidade. O objetivo da associação de várias sub-redes é fornecer alta disponibilidade e redundância de zona de disponibilidade para os clientes. No entanto, a Client VPN não permite dividir o tráfego seletivamente entre as sub-redes associadas ao endpoint da Client VPN.

Os clientes se conectam a um endpoint da Client VPN com base no algoritmo round-robin do DNS. Isso significa que o tráfego pode ser roteado por qualquer uma das sub-redes associadas quando eles estabelecem uma conexão. Portanto, eles poderão enfrentar problemas de conectividade se estiverem em uma sub-rede associada que não tenha as entradas de rota necessárias.

Por exemplo, digamos que você configure as seguintes associações de sub-rede e rotas:

- Associações de sub-rede
  - Associação 1: sub-rede A (us-east-1a)
  - Associação 2: sub-rede B (us-east-1b)
- Rotas
  - Rota 1:10.0.0.0/16 roteada para a sub-rede A
  - Rota 2:172.31.0.0/16 roteada para a sub-rede B

Neste exemplo, os clientes que entrarem na sub-rede A quando se conectarem não poderão acessar a Rota 2, enquanto os clientes que aterrissarem na sub-rede B quando se conectarem não poderão acessar a Rota 1.

Solução

Verifique se o endpoint da Client VPN tem as mesmas entradas de rota com destinos para cada rede associada. Isso garante que os clientes tenham acesso a todas as rotas, independentemente da sub-rede pela qual seu tráfego seja roteado.

Solução de problemas AWS Client VPN: as regras de autorização para grupos do Active Directory não funcionam conforme o esperado

Problema

Configurei regras de autorização para meus grupos do Active Directory, mas elas não estão funcionando como eu esperava. Eu adicionei uma regra de autorização `0.0.0.0/0` para autorizar o tráfego para todas as redes, mas o tráfego ainda falha no destino CIDRs específico.

Causa

As regras de autorização são indexadas na rede CIDRs. As regras de autorização devem conceder aos grupos do Active Directory acesso a uma rede específica CIDRs. As regras de autorização para `0.0.0.0/0` são tratadas como um caso especial e, portanto, são avaliadas por último, independentemente da ordem na qual as regras de autorização são criadas.

Por exemplo, digamos que você crie cinco regras de autorização na seguinte ordem:

- Regra 1: acesso do grupo 1 a `10.1.0.0/16`
- Regra 2: acesso do grupo 1 a `0.0.0.0/0`
- Regra 3: acesso do grupo 2 a `0.0.0.0/0`
- Regra 4: acesso do grupo 3 a `0.0.0.0/0`
- Regra 5: acesso do grupo 2 a `172.131.0.0/16`

Neste exemplo, a regra 2, a regra 3 e a regra 4 são avaliadas por último. O grupo 1 tem acesso somente a `10.1.0.0/16`, e o grupo 2 tem acesso somente a `172.131.0.0/16`. O grupo 3 não tem acesso a `10.1.0.0/16` ou a `172.131.0.0/16`, mas tem acesso a todas as outras redes. Se você remover as regras 1 e 5, todos os três grupos terão acesso a todas as redes.

O cliente VPN usa a correspondência de prefixo mais longa ao avaliar as regras de autorização. Consulte Prioridade de rota no Guia do usuário do Amazon VPC para obter mais detalhes.

Solução

Verifique se você criou regras de autorização que concedam explicitamente aos grupos do Active Directory acesso a uma rede CIDRs específica. Se você adicionar uma regra de autorização para

`0.0.0.0/0`, tenha em mente que ela será avaliada por último e que as regras de autorização anteriores podem limitar as redes às quais ela concede acesso.

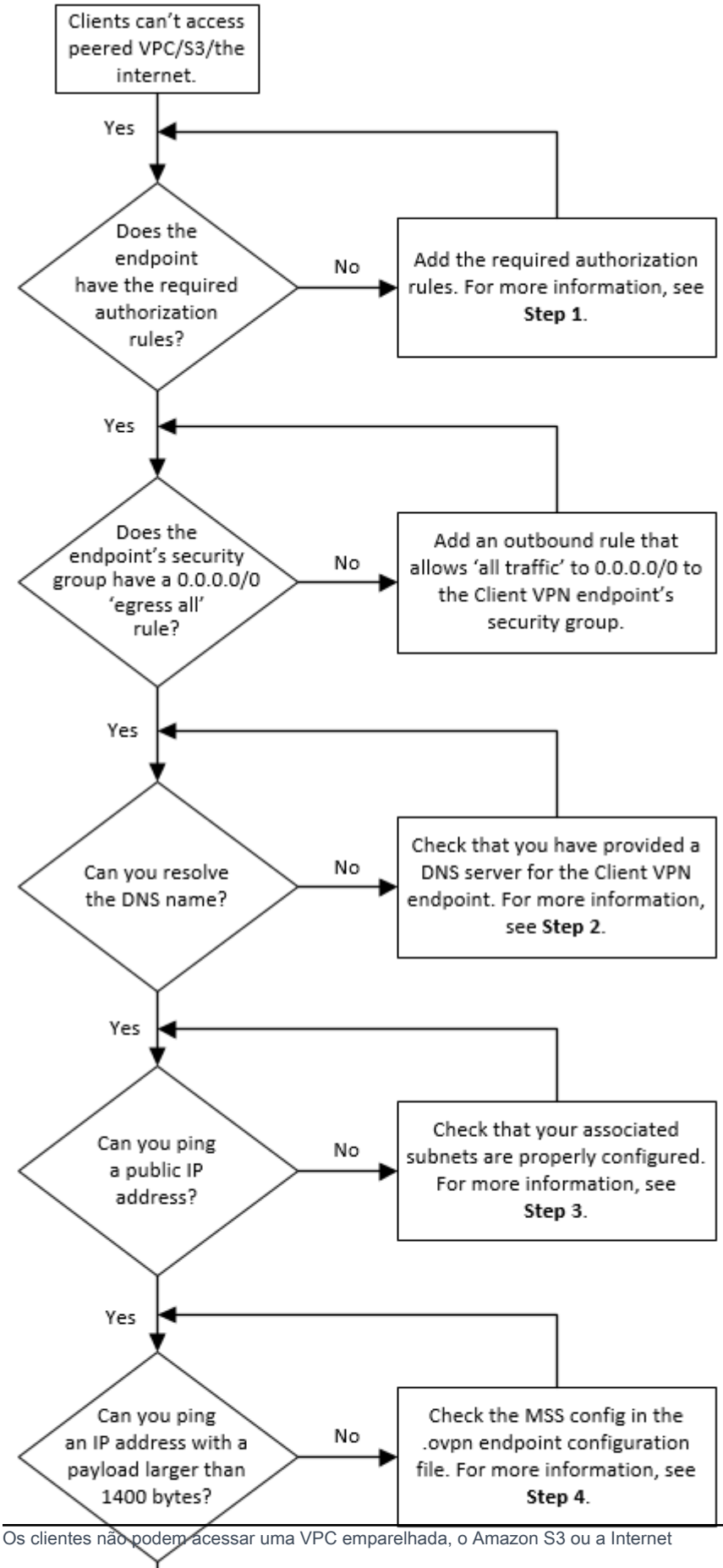
Solução de problemas AWS Client VPN: os clientes não conseguem acessar uma VPC emparelhada, o Amazon S3 ou a Internet

Problema

Configurei corretamente minhas rotas do endpoint da Client VPN, mas meus clientes não conseguem acessar uma VPC emparelhada, o Amazon S3 ou a Internet.

Solução

O fluxograma a seguir contém as etapas para diagnosticar problemas de conectividade da Internet, da VPC emparelhada e do Amazon S3.


Clients can't access peered VPC/S3/the internet.
Yes
Does the endpoint have the required authorization rules?
No
Add the required authorization rules. For more information, see **Step 1**.
Yes
Does the endpoint's security group have a 0.0.0.0/0 'egress all' rule?
No
Add an outbound rule that allows 'all traffic' to 0.0.0.0/0 to the Client VPN endpoint's security group.
Yes
Can you resolve the DNS name?
No
Check that you have provided a DNS server for the Client VPN endpoint. For more information, see **Step 2**.
Yes
Can you ping a public IP address?
No
Check that your associated subnets are properly configured. For more information, see **Step 3**.
Yes
Can you ping an IP address with a payload larger than 1400 bytes?
No
Check the MSS config in the .ovpn endpoint configuration file. For more information, see **Step 4**.
Yes

1. Para acesso à Internet, adicione uma regra de autorização para `0.0.0.0/0`.

   Para acessar uma VPC emparelhada, adicione uma regra de autorização para IPv4 o intervalo CIDR da VPC.

   Para acesso ao S3, especifique o endereço IP do endpoint do Amazon S3.
2. Verifique se é possível resolver o nome DNS.

   Se não for possível resolver o nome DNS, verifique se você especificou os servidores DNS para o endpoint da Client VPN. Se você gerenciar seu próprio servidor DNS, especifique seu endereço IP. Verifique se o servidor DNS é acessível pela VPC.

   Se você não tiver certeza sobre qual endereço IP especificar para os servidores DNS, especifique o resolvedor DNS da VPC no endereço IP .2 na VPC.
3. Para ter acesso à Internet, verifique se você consegue executar ping em um endereço IP público ou em um site público, por exemplo, `amazon.com`. Se não receber uma resposta, certifique-se de que a tabela de rotas para as sub-redes associadas tenha uma rota padrão que tenha como destino um gateway da Internet ou um gateway NAT. Se a rota estiver em vigor, certifique-se de que a sub-rede associada não tenha regras de lista de controle de acesso à rede que bloqueiem o tráfego de entrada e saída.

   Se você não conseguir acessar uma VPC emparelhada, certifique-se de que a tabela de rotas da sub-rede associada tenha uma entrada de rota para a VPC emparelhada.

   Se não conseguir acessar o Amazon S3, certifique-se de que a tabela de rotas da sub-rede associada tenha uma entrada de rota para o endpoint da VPC do gateway.
4. Verifique se é possível executar ping em um endereço IP público com uma carga maior que 1400 bytes. Use um dos seguintes comandos:

   - Windows

     ```
     C:\> ping  8.8.8.8 -l 1480 -f
     ```

   - Linux

     ```
     $ ping -s 1480 8.8.8.8 -M do
     ```

Se não for possível executar ping em um endereço IP com uma carga útil maior que 1400 bytes, abra o arquivo de configuração `.ovpn` do endpoint da Client VPN usando seu editor de texto preferido e adicione o seguinte.

```
mssfix 1328
```

Solução de problemas AWS Client VPN: o acesso a uma VPC emparelhada, ao Amazon S3 ou à Internet é intermitente

Problema

Tenho problemas de conectividade intermitentes ao me conectar a uma VPC emparelhada, ao Amazon S3 ou à Internet, mas o acesso a sub-redes associadas não foi afetado. Preciso me desconectar e reconectar para resolver os problemas de conectividade.

Causa

Os clientes se conectam a um endpoint da Client VPN com base no algoritmo round-robin do DNS. Isso significa que o tráfego pode ser roteado por qualquer uma das sub-redes associadas quando eles estabelecem uma conexão. Portanto, eles poderão enfrentar problemas de conectividade se estiverem em uma sub-rede associada que não tenha as entradas de rota necessárias.

Solução

Verifique se o endpoint da Client VPN tem as mesmas entradas de rota com destinos para cada rede associada. Isso garante que os clientes tenham acesso a todas as rotas, independentemente da sub-rede associada pela qual o tráfego é roteado.

Por exemplo, digamos que o endpoint da Client VPN tenha três sub-redes associadas (sub-rede A, B e C) e que você queira habilitar o acesso à Internet para seus clientes. Para fazer isso, adicione três rotas `0.0.0.0/0` – uma que tenha como destino cada sub-rede associada:

- Rota 1: `0.0.0.0/0` para a sub-rede A
- Rota 2: `0.0.0.0/0` para a sub-rede B
- Rota 3: `0.0.0.0/0` para a sub-rede C

Solução de problemas AWS Client VPN: o software cliente retorna um erro de TLS ao tentar se conectar ao Client VPN

Problema

Antes, eu podia conectar meus clientes à Client VPN com êxito, mas agora o cliente baseado em OpenVPN retorna um dos seguintes erros quando ele tenta se conectar:

```
TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network
 connectivity)
TLS Error: TLS handshake failed
```

```
Connection failed because of a TLS handshake error. Contact your IT administrator.
```

Possível causa nº. 1

Se você usa autenticação mútua e importou uma lista de revogação de certificados de cliente, a lista de revogação de certificados de cliente pode ter expirado. Durante a fase de autenticação, o endpoint da Client VPN verifica o certificado de cliente em relação à lista de revogação de certificados de cliente importada. Se a lista de revogação de certificados de cliente tiver expirado, não será possível conectar-se ao endpoint da Client VPN.

Solução nº. 1

Verifique a data de expiração da lista de revogação de certificados do cliente usando a ferramenta OpenSSL.

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

A saída exibe a data e a hora de expiração. Se a lista de revogação de certificados do cliente tiver expirado, você deverá criar uma nova e importá-la para o endpoint da Client VPN. Para obter mais informações, consulte AWS Client VPN listas de revogação de certificados de clientes.

Possível causa nº. 2

O certificado do servidor que está sendo usado para o endpoint da Client VPN expirou.

Solução nº. 2

Verifique o status do seu certificado de servidor no AWS Certificate Manager console ou usando a AWS CLI. Se o certificado do servidor estiver expirado, crie outro certificado e faça upload para o ACM. Para obter as etapas detalhadas de geração dos certificados e das chaves de servidor e cliente usando o utilitário easy-rsa do OpenVPN e obter instruções sobre como importá-los para o ACM, consulte Autenticação mútua em AWS Client VPN.

Como alternativa, pode haver um problema com o software baseado em OpenVPN que o cliente está usando para se conectar à Client VPN. Para obter mais informações sobre a solução de problemas de software baseado em OpenVPN, consulte Solução de problemas de conexão do cliente VPN no Guia do usuário do AWS Client VPN .

Solução de problemas AWS Client VPN: o software cliente retorna erros de nome de usuário e senha — autenticação do Active Directory

Problema

Uso a autenticação do Active Directory para meu endpoint da Client VPN e antes podia conectar meus clientes à Client VPN com êxito. Mas agora, os clientes estão recebendo erros de nome de usuário e senha inválidos.

Possíveis causas

Se usar a autenticação do Active Directory e se tiver habilitado a autenticação multifator (MFA) depois de distribuir o arquivo de configuração do cliente, o arquivo não conterá as informações necessárias para pedir aos usuários que insiram o código da MFA. Os usuários são solicitados a inserir o nome de usuário e a senha, mas há falha na autenticação.

Solução

Baixe um novo arquivo de configuração do cliente e distribua-o para seus clientes. Verifique se o novo arquivo contém a seguinte linha:

```
static-challenge "Enter MFA code " 1
```

Para obter mais informações, consulte AWS Client VPN exportação do arquivo de configuração do endpoint. Teste a configuração de MFA para o Active Directory sem usar o endpoint da Client VPN para verificar se a MFA está funcionando conforme o esperado.

Solução de problemas AWS Client VPN: o software cliente retorna erros de nome de usuário e senha — autenticação federada

Problema

Tentar fazer login com um nome de usuário e senha com autenticação federada e receber o erro “As credenciais recebidas estavam incorretas. Entre em contato com seu administrador de TI."

Causa

Esse erro pode ser causado por não ter pelo menos um atributo incluído na resposta SAML do IdP.

Solução

Certifique-se de que pelo menos um atributo esteja incluído na resposta SAML do IdP. Consulte Recursos de configuração de IdPs baseados em SAML para obter mais informações.

Solução de problemas AWS Client VPN: os clientes não conseguem se conectar — autenticação mútua

Problema

Uso autenticação mútua para o meu endpoint da Client VPN. Os clientes estão recebendo erros de falha na negociação de chave TLS e erros de tempo limite.

Possíveis causas

O arquivo de configuração que foi fornecido aos clientes não contém o certificado do cliente e a chave privada do cliente ou o certificado e a chave estão incorretos.

Solução

Certifique-se de que o arquivo de configuração contenha o certificado e a chave do cliente corretos. Se necessário, corrija o arquivo de configuração e redistribua-o para seus clientes. Para obter mais informações, consulte AWS Client VPN exportação do arquivo de configuração do endpoint.

Solução de problemas AWS Client VPN: o cliente retorna um erro de credenciais que excedem o tamanho máximo no Client VPN — autenticação federada

Problema

Uso autenticação federada para meu endpoint da Client VPN. Quando os clientes inserem o nome de usuário e a senha na janela do navegador do provedor de identidades (IdP) baseado em SAML, eles recebem um erro informando que as credenciais excedem o tamanho máximo permitido.

Causa

A resposta SAML retornada pelo IdP excede o tamanho máximo permitido. Para obter mais informações, consulte Requisitos e considerações para autenticação federada baseada em SAML.

Solução

Tente reduzir o número de grupos aos quais o usuário pertence no IdP e tente se conectar novamente.

Solução de problemas AWS Client VPN: o cliente não abre o navegador para um endpoint — autenticação federada

Problema

Uso autenticação federada para meu endpoint da Client VPN. Quando os clientes tentam se conectar ao endpoint, o software cliente não abre uma janela do navegador e, em vez disso, exibe uma janela pop-up de nome de usuário e senha.

Causa

O arquivo de configuração fornecido aos clientes não contém o sinalizador `auth-federate`.

Solução

Exporte o arquivo de configuração mais recente, importe-o para o cliente AWS fornecido e tente se conectar novamente.

Solução de problemas AWS Client VPN: o cliente retorna erro sem portas disponíveis — autenticação federada

Problema

Uso autenticação federada para meu endpoint da Client VPN. Quando os clientes tentam se conectar ao endpoint, o software cliente retorna o seguinte erro:

```
The authentication flow could not be initiated. There are no available ports.
```

Causa

O cliente AWS fornecido requer o uso da porta TCP 35001 para concluir a autenticação. Para obter mais informações, consulte Requisitos e considerações para autenticação federada baseada em SAML.

Solução

Verifique se o dispositivo do cliente não está bloqueando a porta TCP 35001 ou a está usando para um processo diferente.

Solução de problemas AWS Client VPN: uma conexão é encerrada devido a uma incompatibilidade de IP

Problema

A conexão VPN foi encerrada e o software-cliente retorna o seguinte erro: `"The VPN connection is being terminated due to a discrepancy between the IP address of the connected server and the expected VPN server IP. Please contact your network administrator for assistance in resolving this issue."`

Causa

O cliente AWS fornecido exige que o endereço IP ao qual ele está conectado corresponda ao IP do servidor VPN que dá suporte ao endpoint do Client VPN. Para obter mais informações, consulte Regras e práticas recomendadas para utilizar o AWS Client VPN.

Solução

Verifique se não há proxy DNS entre o cliente AWS fornecido e o endpoint do Client VPN.

Solução de problemas AWS Client VPN: o tráfego de roteamento para a LAN não está funcionando conforme o esperado

Problema

A tentativa de rotear o tráfego para a rede local (LAN) não funciona conforme o esperado quando os intervalos de endereço IP da LAN não estão dentro dos seguintes intervalos de endereço IP privados padrão: `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16` ou `169.254.0.0/16`.

Causa

Se for detectado que o intervalo de endereços da LAN do cliente está fora dos intervalos padrão acima, o endpoint da Client VPN enviará automaticamente a diretiva OpenVPN “redirect-gateway block-local” para o cliente, forçando todo o tráfego da LAN para a VPN. Para obter mais informações, consulte Regras e práticas recomendadas para utilizar o AWS Client VPN.

Solução

Se você precisar de acesso à LAN durante as conexões VPN, é recomendável usar os intervalos de endereços convencionais listados acima para sua LAN.

Solução de problemas AWS Client VPN: verifique o limite de largura de banda para um endpoint Client VPN

Problema

Preciso verificar o limite de largura de banda para um endpoint da Client VPN.

Causa

A taxa de transferência depende de vários fatores, como a capacidade da conexão do local e a latência da rede entre a aplicação para desktop de Client VPN no computador e o VPC endpoint. Uma largura de banda mínima de 10 Mbps é suportada por conexão de usuário.

Solução

Execute os comandos a seguir para verificar a largura de banda.

```
sudo iperf3 -s -V
```

No cliente:

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

Solução de problemas AWS Client VPN: problemas de conectividade de túnel com uma VPC

Ao enfrentar problemas de conectividade com sua AWS Client VPN conexão, siga esta abordagem sistemática de solução de problemas para identificar e resolver o problema. Esta seção fornece step-by-step procedimentos para diagnosticar problemas comuns de conectividade do Client VPN entre clientes remotos e recursos da Amazon VPC.

Tópicos

- Pré-requisitos de conectividade de rede
- Verifique o status do endpoint do Client VPN
- Verifique as conexões do cliente
- Verifique a autenticação do cliente
- Verifique as regras de autorização
- Validar rotas do Client VPN
- Verifique os grupos de segurança e a rede ACLs
- Teste a conectividade do cliente
- Diagnosticar o dispositivo cliente
- Solucionar problemas de resolução de DNS
- Solucionar problemas de desempenho
- Monitore as métricas do Client VPN
- Verifique os registros do Client VPN
- Problemas e soluções comuns de

Pré-requisitos de conectividade de rede

Antes de solucionar problemas de conectividade do Client VPN, verifique estes pré-requisitos de rede:

- Certifique-se de que a sub-rede do endpoint do Client VPN tenha conectividade com a Internet (via Internet Gateway ou NAT Gateway).

- Verifique se o endpoint do Client VPN está associado a sub-redes em diferentes zonas de disponibilidade para obter alta disponibilidade.
- Verifique se a VPC tem espaço de endereço IP suficiente e não está em conflito com os blocos CIDR do cliente.
- Confirme se as sub-redes de destino têm associações de tabela de rotas adequadas.

Verifique o status do endpoint do Client VPN

Primeiro, verifique se o endpoint do Client VPN está no estado correto:

1. Use o AWS CLI para verificar o status do endpoint do Client VPN:

```
aws ec2 describe-client-vpn-endpoints --region your-region
```

2. Procure o estado do endpoint na saída. O estado deveria ser`available`.
3. Verifique se o endpoint tem redes de destino associadas (sub-redes).
4. Se o estado não for`available`, verifique se há mensagens de erro ou estados pendentes que possam indicar problemas de configuração.

Verifique as conexões do cliente

Verifique o status das conexões do cliente com seu endpoint do Client VPN:

1. Verifique as conexões ativas do cliente:

```
aws ec2 describe-client-vpn-connections --client-vpn-endpoint-id cvpn-endpoint-id
 --region your-region
```

2. Revise o status da conexão e todas as mensagens de erro na saída.
3. Verifique os registros de autenticação do cliente em busca de tentativas de autenticação malsucedidas.
4. Verifique se os clientes estão recebendo endereços IP do bloco CIDR do cliente configurado.

> **Note**
>
> Se os clientes não conseguirem se conectar, o problema provavelmente está na configuração de autenticação, nas regras de autorização ou na conectividade de rede.

Verifique a autenticação do cliente

Problemas de autenticação são causas comuns de problemas de conectividade do Client VPN:

- Para autenticação mútua, certifique-se de que os certificados do cliente sejam válidos e não tenham expirado.
- Para autenticação do Active Directory, verifique as credenciais do usuário e a conectividade do domínio.
- Para autenticação federada baseada em SAML, verifique a configuração do IdP e as permissões do usuário.
- Revise os registros de autenticação CloudWatch para obter informações detalhadas sobre erros.
- Verifique se o método de autenticação configurado no endpoint corresponde à configuração do cliente.

Verifique as regras de autorização

As regras de autorização controlam quais recursos de rede os clientes podem acessar:

1. Liste as regras de autorização atuais:

   ```
   aws ec2 describe-client-vpn-authorization-rules --client-vpn-endpoint-id cvpn-endpoint-id --region your-region
   ```

2. Verifique se existem regras para as redes de destino que os clientes precisam acessar.
3. Verifique se as regras especificam os grupos corretos do Active Directory (se estiver usando a autenticação AD).
4. Certifique-se de que as regras de autorização estejam em `active` vigor.

Validar rotas do Client VPN

A configuração de roteamento adequada é essencial para a conectividade do Client VPN:

1. Verifique as rotas dos endpoints do Client VPN:

```
aws ec2 describe-client-vpn-routes --client-vpn-endpoint-id cvpn-endpoint-id --
region your-region
```

2. Verifique se existem rotas para as redes de destino que os clientes precisam acessar.
3. Verifique as tabelas de rotas do Amazon VPC para garantir que o tráfego de retorno possa alcançar o endpoint do Client VPN:

```
aws ec2 describe-route-tables --filters "Name=vpc-id,Values=vpc-id" --region your-
region
```

4. Verifique se as associações de rede de destino estão configuradas corretamente.

Verifique os grupos de segurança e a rede ACLs

Os grupos de segurança e a rede ACLs podem bloquear o tráfego do Client VPN:

1. Verifique os grupos de segurança das EC2 instâncias de destino:

```
aws ec2 describe-security-groups --group-ids sg-xxxxxxxxx --region your-region
```

2. Verifique se as regras de entrada permitem o tráfego do bloco CIDR do Client VPN:
   - SSH (porta 22) do Client VPN CIDR: `10.0.0.0/16`
   - HTTP (porta 80) do Client VPN CIDR: `10.0.0.0/16`
   - HTTPS (porta 443) do Client VPN CIDR: `10.0.0.0/16`
   - Portas de aplicativos personalizadas conforme necessário
3. Para o grupo de segurança de endpoint do Client VPN (se aplicável), verifique se ele permite:
   - Porta UDP 443 (OpenVPN) de 0.0.0.0/0
   - Todo o tráfego de saída para blocos CIDR da VPC
4. Verifique se a rede não ACLs está bloqueando o tráfego. A rede ACLs não tem estado, portanto, as regras de entrada e saída devem ser configuradas.

5. Verifique as regras de entrada e saída para o tráfego específico que você está tentando enviar.

Teste a conectividade do cliente

Teste a conectividade dos clientes Client VPN com os recursos da Amazon VPC:

1. Em um cliente Client VPN conectado, teste a conectividade com os recursos da Amazon VPC:

```
ping vpc-resource-ip
traceroute vpc-resource-ip
```

2. Teste a conectividade específica do aplicativo:

```
telnet vpc-resource-ip port
```

3. Verifique a resolução do DNS se estiver usando nomes DNS privados:

```
nslookup private-dns-name
```

4. Teste a conectividade com os recursos da Internet se o tunelamento dividido estiver ativado.

Diagnosticar o dispositivo cliente

Execute estas verificações no dispositivo cliente:

1. Verifique se o arquivo de configuração do cliente (.ovpn) contém as configurações corretas:
   - URL correta do endpoint do servidor
   - Certificado de cliente e chave privada válidos
   - Configuração adequada do método de autenticação
2. Verifique se há erros de conexão nos registros do cliente:
   - Windows: Visualizador de eventos → Registros de aplicativos e serviços → OpenVPN
   - macOS: aplicativo de console, pesquise por “Tunnelblick” ou “OpenVPN”
   - Linux: `/var/log/openvpn/` ou diário systemd
3. Teste a conectividade básica de rede do cliente:

```
ping 8.8.8.8
```

```
nslookup cvpn-endpoint-id.cvpn.region.amazonaws.com
```

Solucionar problemas de resolução de DNS

Problemas de DNS podem impedir o acesso a recursos usando nomes DNS privados:

1. Verifique se os servidores DNS estão configurados no endpoint do Client VPN:

```
aws ec2 describe-client-vpn-endpoints --client-vpn-endpoint-ids cvpn-endpoint-id --
query 'ClientVpnEndpoints[0].DnsServers'
```

2. Teste a resolução de DNS do cliente:

```
nslookup private-resource.internal
dig private-resource.internal
```

3. Verifique as regras do Route 53 Resolver se estiver usando uma resolução de DNS personalizada.
4. Verifique se os grupos de segurança permitem tráfego DNS (porta UDP/TCP 53) do Client VPN CIDR para servidores DNS.

Solucionar problemas de desempenho

Solucione problemas de desempenho com conexões Client VPN:

- Monitore a utilização da largura de banda usando CloudWatch métricas para ingress/egress bytes.
- Verifique a perda de pacotes usando testes de ping contínuos dos clientes.
- Verifique se o endpoint do Client VPN não está atingindo os limites de conexão.
- Considere o uso de vários endpoints do Client VPN para distribuição de carga.
- Teste com diferentes locais de clientes para identificar problemas de desempenho regional.

Monitore as métricas do Client VPN

Monitore as métricas de endpoint do Client VPN usando CloudWatch:

1. Verifique as métricas de conexão ativa:

```
aws cloudwatch get-metric-statistics \
  --namespace AWS/ClientVPN \
  --metric-name ActiveConnectionsCount \
  --dimensions Name=Endpoint,Value=cvpn-endpoint-id \
  --start-time start-time \
  --end-time end-time \
  --period 300 \
  --statistics Average
```

2. Analise as métricas de falha de autenticação:

```
aws cloudwatch get-metric-statistics \
  --namespace AWS/ClientVPN \
  --metric-name AuthenticationFailures \
  --dimensions Name=Endpoint,Value=cvpn-endpoint-id \
  --start-time start-time \
  --end-time end-time \
  --period 300 \
  --statistics Sum
```

3. Analise outras métricas disponíveis, como bytes e pacotes de entrada e saída.

Verifique os registros do Client VPN

Os registros de conexão do Client VPN fornecem informações detalhadas sobre tentativas e erros de conexão:

- Ative o registro de conexão do Client VPN se ainda não estiver configurado.
- Analise CloudWatch os registros de tentativas de conexão, falhas de autenticação e erros de autorização.
- Procure códigos de erro e mensagens específicos que indiquem a causa raiz dos problemas de conectividade.
- Verifique se há padrões em conexões com falha que possam indicar problemas de configuração.

Problemas e soluções comuns de

Problemas comuns que podem afetar a conectividade do Client VPN:

Falhas de autenticação

Certificados de cliente expirados ou inválidos, ou credenciais do Active Directory incorretas. Verifique a configuração da autenticação e a validade da credencial.

Regras de autorização ausentes

Os clientes não podem acessar as redes de destino devido a regras de autorização ausentes ou incorretas. Adicione regras de autorização apropriadas para as redes necessárias.

Problemas de tunelamento dividido

Roteamento de tráfego incorreto devido à configuração de tunelamento dividido. Revise e ajuste as configurações de tunelamento dividido conforme necessário.

Exaustão do pool IP do cliente

Não há endereços IP disponíveis no bloco CIDR do cliente. Expanda o intervalo CIDR do cliente ou desconecte clientes não utilizados.

Problemas de MTU

Pacotes grandes estão sendo descartados devido às limitações de tamanho da MTU. Tente definir a MTU para 1436 bytes ou habilitar o Path MTU Discovery em dispositivos cliente.

Problemas de resolução de DNS

Os clientes não conseguem resolver nomes DNS privados. Verifique a configuração do servidor DNS e garanta que o tráfego DNS seja permitido por meio de grupos de segurança.

Intervalos de IP sobrepostos

O CIDR do cliente bloqueia conflitos com intervalos de rede local. Verifique e resolva quaisquer intervalos de endereços IP sobrepostos entre o CIDR do cliente e as redes locais.

Falhas no handshake do TLS

A conexão falha durante a negociação do TLS. Verifique a validade do certificado, garanta os conjuntos de criptografia corretos e verifique se os certificados de cliente e servidor estão configurados corretamente.

Atrasos na propagação da rota

Novas rotas não estão imediatamente disponíveis para os clientes. Aguarde de 1 a 2 minutos para a propagação da rota depois de fazer alterações nas rotas do Client VPN.

Quedas de conexão/instabilidade

Desconexões frequentes ou conexões instáveis. Verifique se há congestionamento de rede, interferência de firewall ou configurações de gerenciamento de energia nos dispositivos cliente.

Histórico do documento do Guia do usuário da Client VPN

A tabela a seguir descreve as atualizações do Guia AWS Client VPN do Administrador.

Alteração	Descrição	Data
Recurso de fiscalização de rotas do cliente	Adição do recurso de fiscalização de rotas do cliente.	20 de abril de 2025
Aumento da cota de Client VPN	Aumentamos a cota de regras de autorização por endpoint do Client VPN de 50 para 200.	13 de março de 2025
Support para desconexão no tempo limite da sessão	O tempo limite da sessão agora permite a desconexão quando a duração máxima da sessão é atingida.	13 de janeiro de 2025
Aumento das cotas	As cotas para regras de autorização por endpoint Client VPN e Routes por endpoint Client VPN aumentaram de 50 e 10, respectivamente, para 100.	19 de dezembro de 2024
Exemplo de regras de autorização	Adição de cenários de exemplo para regras de autorização.	15 de setembro de 2022
Duração máxima da sessão VPN	É possível configurar uma duração máxima de sessão VPN menor para atender aos requisitos de segurança e conformidade.	20 de janeiro de 2022
Banner de login do cliente	Você pode ativar um banner de texto nos aplicativos de desktop Client VPN	20 de janeiro de 2022

	AWS fornecidos quando uma sessão de VPN for estabelecida para atender às necessidades regulatórias e de conformidade.	
Manipulador de conexão do cliente	É possível habilitar o manipulador de conexão do cliente para seu endpoint da Client VPN para executar uma lógica personalizada que autoriza novas conexões.	4 de novembro de 2020
Portal de autoatendimento	É possível habilitar um portal de autoatendimento em seu endpoint da Client VPN para seus clientes.	29 de outubro de 2020
Client-to-client access	Você pode permitir que clientes que se conectam a um endpoint do Client VPN se conectem entre si.	29 de setembro de 2020
Autenticação federada baseada em SAML 2.0	É possível autenticar usuários da Client VPN usando a autenticação federada baseada em SAML 2.0.	19 de maio de 2020
Especificar grupos de segurança durante a criação	É possível especificar uma VPC e grupos de segurança ao criar o endpoint do AWS Client VPN .	5 de março de 2020
Portas VPN configuráveis	Você pode especificar um número de porta VPN compatível para seu AWS Client VPN endpoint.	16 de janeiro de 2020

Compatibilidade com autenticação multifator (MFA)	Seu AWS Client VPN endpoint oferece suporte ao MFA se estiver habilitado para o Active Directory.	30 de setembro de 2019
Compatibilidade com túnel dividido	Você pode ativar o túnel dividido em seu endpoint. AWS Client VPN	24 de julho de 2019
Lançamento inicial	Essa versão apresenta o AWS Client VPN.	18 de dezembro de 2018

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.